



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

---

J-6

DISTRIBUTION: A, B, C, J

CJCSI 6212.01B

8 May 2000

## INTEROPERABILITY AND SUPPORTABILITY OF NATIONAL SECURITY SYSTEMS, AND INFORMATION TECHNOLOGY SYSTEMS

References: See Enclosure F

1. Purpose. This instruction:

a. Establishes policies and procedures for the J-6 interoperability requirements certification of mission need statements (MNSs), Capstone Requirements Documents (CRDs), and operational requirements documents (ORDs) required by reference a.

b. Details a methodology to develop interoperability key performance parameters (KPPs) derived from a set of top-level information exchange requirements (IERs) as required by reference a and based on the format and content of the integrated architecture products described in the C4ISR Architecture Framework (reference h).

c. Establishes policies and procedures for the J-6 supportability certification of command, control, communications, computers, and intelligence (C4I) support plans (C4ISPs).

d. Establishes policies and procedures for the J-6 interoperability system validation.

2. Cancellation. CJCSI 6212.01A, 30 June 1995, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems," is canceled.

3. Applicability

a. This instruction applies to the Joint Staff, Services, unified commands, and those DOD field activities and Defense agencies

## Report Documentation Page

<b>Report Date</b> 08052000	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> -
<b>Title and Subtitle</b> Interoperability	<b>Contract Number</b>	
	<b>Grant Number</b>	
	<b>Program Element Number</b>	
<b>Author(s)</b>	<b>Project Number</b>	
	<b>Task Number</b>	
	<b>Work Unit Number</b>	
<b>Performing Organization Name(s) and Address(es)</b> Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102	<b>Performing Organization Report Number</b>	
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b> Chariman of the Joint Chiefs of Staff	<b>Sponsor/Monitor's Acronym(s)</b>	
	<b>Sponsor/Monitor's Report Number(s)</b>	
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b> The original document contains color images.		
<b>Abstract</b>		
<b>Subject Terms</b> IATAC COLLECTION		
<b>Report Classification</b> unclassified	<b>Classification of this page</b> unclassified	
<b>Classification of Abstract</b> unclassified	<b>Limitation of Abstract</b> UU	
<b>Number of Pages</b> 101		

8 May 2000

supporting the defense acquisition responsibilities of the Chairman of the Joint Chiefs of Staff. This instruction also applies, in general, to other agencies preparing and submitting requirements IAW references b and c.

b. Highly sensitive classified programs will comply with this instruction, but will be tailored to account for special security considerations (reference b, part I, paragraph 1.4, and reference c, page 2).

c. This instruction does not preclude the need to refer to reference a, "Requirements Generation System," and the basic DOD 5000 series documents for guidance and direction on defense acquisition. All DOD components responsible for generating requirements documents will base their respective procedures for ACAT II and below programs on those contained in reference a.

4. Scope. This instruction addresses the interoperability and supportability of new National Security Systems (NSS) and information technology systems (ITS) or modifications to existing systems regardless of ACAT. NSS and ITS are defined in Part II of the Glossary. Intelligence supportability is addressed in a separate, but related, process conducted by the J-2. This instruction considers automated information systems (AISs) to be an ITS.

## 5. Policy

### a. National Security Systems and Information Technology Systems Development

(1) For purposes of interoperability and supportability, all NSS and ITS developed for use by US forces are for joint (references d and e), combined, and coalition use. Interoperability and supportability of NSS and ITS requirements will be determined during the requirements validation process and will be updated as necessary throughout the acquisition period, deployment, and operational life of a system (reference a).

(2) The overall objective of this policy decision is to develop, acquire, and deploy NSS and ITS that (1) meet the essential operational needs of US forces; (2) are interoperable with existing and proposed NSS and ITS; (3) are supportable over the existing and planned global information grid; and (4) are interoperable with allies and coalition partners.

b. J-6 Certification and Validation Process. Figure 1 below illustrates the two J-6 certifications and one J-6 validation discussed in the

8 May 2000

following paragraphs. J-2 certification of intelligence supportability related to, but has distinctions from procedures in this instruction.

(1) J-6 Interoperability Requirements Certification. This certification occurs prior to each acquisition milestone (0, I, II, III).

(a) The J-6 certifies MNSs, CRDs, and ORDs, regardless of ACAT level, for conformance with joint NSS and ITS policy, doctrine, and interoperability standards. The J-6 also certifies the interoperability KPP derived from a set of top-level IERs. As part of the review process, J-6 requests assessments from the Services, Defense Information Systems Agency (DISA), and DOD agencies.

(b) CINCs are required to review and comment on ACAT I/IA and Joint Requirements Oversight Council (JROC) special interest requirements documents during the J-8 JROC formal review. CINCs are provided the opportunity to review and comment on ACAT II and below documents during the J-6 interoperability requirements certification process.

(c) USJFCOM, as the joint force integrator, will review and confirm sufficiency of interoperability KPPs and IER matrices for all CRDs and ORDs regardless of ACAT.

(d) The J-6 forwards interoperability requirements certification to the JROC for ACAT I/IA and JROC special interest programs or to the sponsoring DOD component for ACAT II and below programs. Also, J-6 forwards unresolved interoperability issues to the Military Communications-Electronics Board (MCEB) or Military Intelligence Board (MIB) for resolution.

(e) The MCEB or MIB will return resolved interoperability issues to the lead DOD component so it may complete JROC approval process. The MCEB and MIB will ensure that unresolved issues

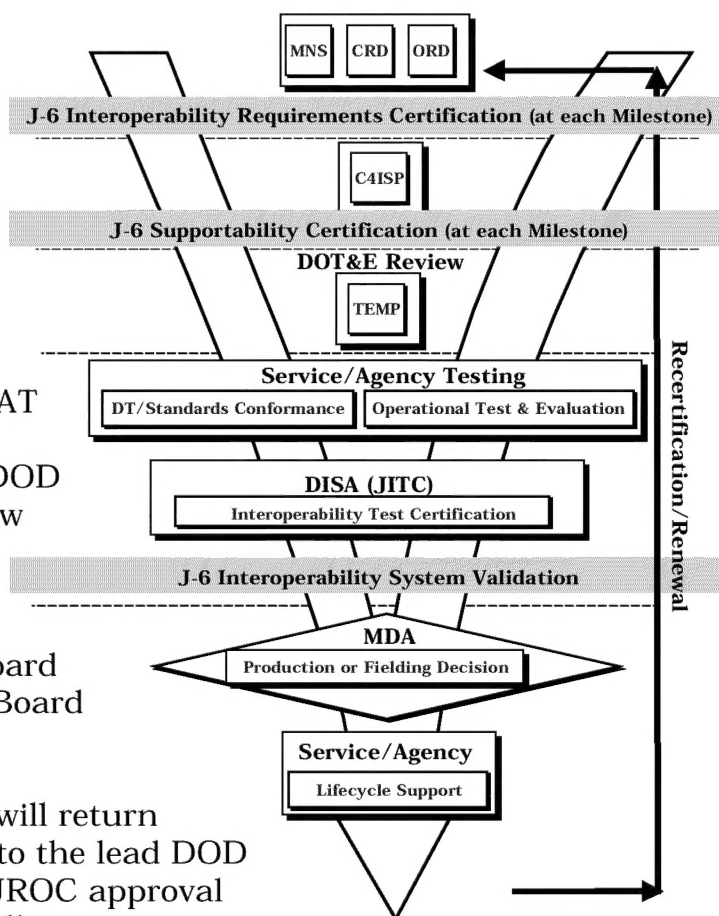


Figure 1 J-6 Certification and Validation Process

8 May 2000

resulting from interoperability assessments are presented to the JROC for resolution or further action (see Enclosure D, Figure D-1).

(2) J-6 Supportability Certification. The J-6 certifies to ASD(C3I) that C4ISPs, regardless of ACAT, adequately address NSS and ITS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems. As part of the review process, J-6 requests supportability assessments from DISA and DOD agencies. CINCs are provided the opportunity to review and comment on documents, regardless of ACAT, during the J-6 supportability certification process. J-6 conducts a supportability certification for C4ISPs prior to Milestone I, II, and III for submission to ASD(C3I) as part of the C4ISP review process. In a separate, but related process, the J-2 provides an intelligence supportability certification.

(3) J-6 Interoperability System Validation. The J-6 validation is intended to provide total life-cycle oversight of warfighter interoperability requirements. The J-6 validates that the interoperability KPP derived from the set of top-level IERs approved in the CRD (if applicable), ORD, and C4ISP was adequately tested and testing results certified during the DISA (JITC) interoperability system test certification. Fifteen days after receipt of the DISA (JITC) interoperability system test certification memorandum (described in paragraph c below), the J-6 will issue an interoperability system validation memorandum to the respective Services, agencies, and developmental and operational testing organizations.

c. Interoperability Testing and Test Certification

(1) All NSS and ITS, regardless of ACAT, must be tested and testing results certified by DISA (JITC). Testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early user test) whenever possible to conserve resources. Interoperability evaluation and testing will be conducted throughout the life cycle of NSS and ITS and interfaces. See Appendix B to Enclosure D for a description of the interoperability system test and certification process.

(2) Interoperability testing and test certification must be addressed as an integral part of the requirements generation process prior to production and fielding approval (if not sooner) by the milestone decision authority (MDA) at all ACAT levels.

(3) Standards conformance testing, as well as interoperability interface testing, will be planned and conducted during the development

8 May 2000

and acquisition of the system with the systems being certified in writing by DISA (JITC) prior to each program's milestone decision.

(4) Hardware and software modifications that affect interoperability of fielded NSS and ITS will require DISA (JITC) recertification before the modifications are fielded for initial operational capability (IOC).

d. Interoperability Policy and Test Panel

(1) MCEB Interoperability Policy and Test Panel (IPTP) resolves issues in joint testing and interoperability certification. Intelligence interoperability issues will be referred to the MIB.

(2) A temporary waiver from interoperability system testing certification -- an Interim Authority to Operate (IATO) -- may be granted by the IPTP in special situations.

(3) Submit requests for an IATO to the IPTP IAW reference f (or see the DISA (JITC)/IPTP website: <http://jitc.fhu.disa.mil>).

(4) IATOs will not to exceed 1 year.

e. Interoperability Testing and Test Certification Programming and Budgeting

(1) CINCs, Services, and agencies (C/S/As) are generally responsible for funding interoperability testing for systems that have not reached IOC. Required interoperability testing and certification will impact schedule and program cost and will need to be added to POM and program cost estimates.

(2) C/S/A may designate and fund another C/S/A test organization to conduct interoperability testing.

(3) When DISA (JITC) is not the interoperability testing organization, interoperability test plans, test analysis, and test reports will be coordinated with and approved by DISA (JITC) to ensure sufficient information is available to allow DISA (JITC) to certify a system. Tests and certifications are scheduled by DISA (JITC), with a balance between the program manager's schedule, DISA (JITC)'s available test resources, organizational priorities, and functional priorities.

f. Interoperability Testing and Test Certification Prioritization.  
C/S/As will incorporate interoperability testing into their overall testing plans in coordination with DISA (JITC).

(1) DISA (JITC) uses the following organizational prioritization for testing, assessing, and certifying interoperability: (1) joint NSS and ITS systems that support the unified commands, (2) joint NSS and ITS systems that are acquired by the Services, and (3) systems that are acquired by the Defense agencies.

(2) The order for functional prioritization is: (1) tactical and strategic warning and communications that support the unified commands and the National Command Authorities (NCA); (2) C2 systems that support the unified commands; (3) intelligence systems that support the unified commands; and (4) combat service support systems that support the unified commands.

(3) The proposed DISA (JITC) interoperability testing and test certification schedule will be submitted to the ITP for review and approval. Any conflicts in schedules, testing resources, or priorities are resolved by the ITP, if possible. Issues that cannot be resolved by the ITP process will be brought to the attention of the MCEB for final resolution.

(4) The interoperability test certification prioritization process is intended as a positive enhancement to overall system development and should not impede, delay, or restrict individual system milestone accomplishment as a result of a lack of testing resources. Should test delays occur as a result of the lack of tester resources, then test waivers should be submitted to the ITP.

g. Standardized Test Plans. DISA develops standardized test plans and procedures in coordination with the Services and agencies for conducting standards conformance testing, interoperability testing, and certification of specific categories or classes of NSS and ITS systems. The standardized test plans and procedures for conducting interoperability system test certification are available from DISA (JITC).

h. Information Technology Standards. New or modified NSS and ITS systems should be standards-based. NSS and ITS must comply with applicable information technology standards contained in the current DOD Joint Technical Architecture (JTA) (reference g is available at <http://www-jta.ncr.disa.mil>).

i. NSS and ITS System-specific Policies. Current and newly established interoperability related policies that impact J-6 certifications are detailed in Enclosure E.

j. Interoperability Key Performance Parameter (KPP)

(1) CJCSI 3170.01A (reference a) requires CRDs and ORDs to contain an interoperability KPP that is derived from the set of top-level information IERs that characterize the information exchanges to be performed by the proposed family of systems (FoS)/system of systems (SoS) or system.

(a) For CRDs, top-level IERs are defined as those information exchanges that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS (i.e., with other C/S/A, allied, and coalition systems).

(b) For ORDs, top-level IERS are defined as those information exchanges that are external to the system (i.e., with other C/S/A, allied, and coalition systems).

(2) Top-level IERs are derived from a high-level operational concept graphic and a system interface description that illustrate the proposed system's information exchange requirements for mission accomplishment.

(a) Top-level IERs at the CRD level do not impose, nor should they be construed as imposing, any specific material solution. CRD top-level IERs are designed to identify the basic characteristics of the information that needs to be exchanged between C/S/A, allies, and coalition partners in order to accomplish the mission.

(b) IERs are described in a matrix format.

(c) CRD Interoperability KPPs, and hence the IERs that the Interoperability KPPs are derived from, will be measurable.

(d) ORD Interoperability KPPs, and hence the IERs that the interoperability KPPs are derived from, will be measurable and testable.

(3) The interoperability KPP, along with other KPPs and critical technical and operational issues, is used to develop the C4ISP and the test and evaluation master plan (TEMP). A methodology to develop CRD and ORD interoperability KPPs, based on the procedures described in the C4ISR Architecture Framework (reference h) is detailed in Enclosure B.

6. Implementation and Supplementation. This instruction will not be supplemented without the prior approval of the Vice Chairman of the Joint Chiefs of Staff or his delegated representative.

7. Abbreviations, Acronyms, and Definitions. See the Glossary.

8 May 2000

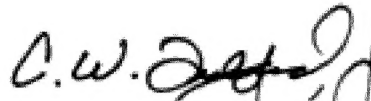
8. Responsibilities. See Enclosure A.

9. Summary of Changes. Major changes reflect revisions to reference a. A methodology to develop CRD and ORD interoperability KPPs required by reference a is detailed in Enclosure B. MNS, CRD, and ORD assessment criteria matrices were updated, and C4ISP assessment criteria matrix were added. J-6 assessment tool procedures, J-6 supportability certification, and NSS and ITS specific policies were added. C4I for the Warrior was deleted.

10. Effective Date. This instruction is effective upon receipt.

11. Releasability. This instruction is approved for public release and distribution is unlimited. DOD components (to include the combat commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page -- <http://www.dtic.mil/doctrine/jel/cjcsd.htm>. Copies are also available through the Government Printing Office on the Electronic Library CD-ROM.

For the Chairman of the Joint Chiefs of Staff:



C.W. FULFORD, JR  
Lieutenant General, U.S. Marine Corps  
Director, Joint Staff

Enclosures:

A--Responsibilities

B--Interoperability Key Performance Parameters and Top-level  
Information Exchange Requirements

C--J-6 Interoperability And Supportability Certification Assessment  
Criteria

Appendix A - Requirements Documents (MNSs, CRDs, ORDs)

Appendix B - C4I Support Plan (C4ISP)

D--Procedures

Appendix A - J-6 Assessment Tool

Appendix B - Interoperability Testing and Test Certification Process

E--NSS and ITS System Specific Policies

F--References

Glossary

## LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 8	O	D-1 thru D-6	O
i thru iv	O	D-A-1 thru D-A-8	O
A-1 thru A-8	O	D-B-1 thru D-B-4	O
B-1 thru B-20	O	E-1 thru E-2	O
C-1 thru C-2	O	F-1 thru F-2	O
C-A-1 thru C-A-12	O	GL-I-1 thru GL-I-6	O
C-B-1 thru C-B-10	O	GL-II-1 thru GL-II-10	O

(INTENTIONALLY BLANK)

## RECORD OF CHANGES

[illegible]

(INTENTIONALLY BLANK)

ENCLOSURE A  
RESPONSIBILITIES

1. The Joint Staff, J-6, will:

- a. Conduct an interoperability requirements certification of MNSs, CRDs, and ORDs, regardless of ACAT level.
- b. Conduct supportability certifications of C4I support plans, regardless of ACAT level.
- c. Conduct interoperability system test validation of all NSS and ITS regardless of ACAT.
- d. Coordinate interoperability and supportability policies, procedures, and programs.
- e. Advise OSD on NSS and ITS interoperability and supportability in the areas of military requirements, research and development (R&D), security assistance, and force planning in concert with J-2, J-3, J-4, J-7, and J-8.
- f. Monitor R&D and acquisition of NSS and ITS in collaboration with J-8.
- g. Convene the MCEB consisting of the senior Service and agency officials responsible for communications-electronics matters and act as chairman (reference f). The MCEB will consider interoperability and supportability matters referred to it by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. The board will:
  - (1) Act as the senior resolution body for issues related to NSS and ITS, standards, and interoperability testing issues.
  - (2) Obtain coordination for issues presented to the board among DOD components, between the Department of Defense and other governmental departments and agencies, and between the Department of Defense and representatives of foreign nations.
  - (3) Coordinate and furnish advice, guidance, direction, and assistance among components for NSS and ITS interoperability and supportability matters.

8 May 2000

(4) Establish the following subpanels whose duties in regards to this instruction are as defined:

(a) The ITP will oversee conduct of the interoperability certification process, resolve testing issues, and waive requirements for interoperability certification.

(b) The information assurance panel (IAP) will resolve information assurance (IA) interoperability issues. This includes IA interoperability requirements between US NSS and ITS and those of allies.

(c) The data systems interoperability panel (DP) will resolve issues involving procedures for tactical information exchange.

(d) The standards coordinating committee (SCC) will resolve standards issues that arise in the MCEB process.

h. Designate a POC to act as the J-6 assessment tool executive agent (see Appendix A, Enclosure D).

2. Joint Staff, J-2, will:

a. Perform intelligence interoperability assessment of MNSs, ORDs, CRDs for all ACATs and forward to the J-6.

b. Designate a J-2 document assessor POC for the J-6 assessment tool (see Appendix A, Enclosure D). There is only one document assessor POC for each organization. The document assessor POC is responsible for identifying who in his/her organization should review a document and for providing the individual the "document assessor" username and password so they can access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.

3. DOD Chief Information Officer (CIO) will:

a. Ensure the interoperability of NSS and ITS throughout the Department of Defense.

b. Prescribe NSS and ITS standards that will apply throughout the Department of Defense.

c. Eliminate duplicate information technology within and between the Military Departments and Defense agencies.

8 May 2000

4. US Joint Forces Command (USJFCOM). As the joint force integrator, USJFCOM will review and confirm the sufficiency of interoperability KPPs and IER matrices for all CRDs and ORDs regardless of ACAT. This evaluation will be based on the warfighter's perspective using a universal joint task list (UJTL)/joint mission-essential task list (JMETL) based assessment process.

5. CINCs will:

a. Review and comment on all ACAT I/IA and JROC special interest documents that are validated and approved by the JROC. CINCs also are provided the opportunity to review and comment on ACAT II and below documents during the J-2 and J-6 certification processes.

b. Designate a CINC document submitter POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization will have only one document submitter POC. The document submitter POC identifies the individual within the organization who is authorized to submit documents on-line, and provides that individual the username and password needed to access the J-6 assessment tool. The document submitter username and password are obtained from J-6I.

c. Designate a CINC document assessor POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization will have only one document assessor POC. The document assessor POC identifies the individual within the organization who should review a document, and provides the individual with the document assessor username and password needed to access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.

d. Participate, as appropriate, in NSS and ITS interoperability testing programs by planning, programming, budgeting, and providing resources IAW agreed-to schedules and test plans. Required interoperability testing and certification will have some impact on schedule and cost of programs. These cost and schedule impacts will need to be added to POM and project cost estimates.

6. Military Services and Defense Agencies will:

a. Designate a Service or agency document submitter POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization will have only one document submitter POC. The document submitter POC identifies the individual authorized to submit documents on-line, and provides that individual with the document submitter username and password needed to access the J-6 assessment tool. The document submitter username and password are obtained from J-6I.

- b. Designate a Service or agency document assessor POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization will have only one document assessor POC. The document assessor POC identifies the individual who reviews a document and provides that individual with the document assessor username and password needed to access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.
- c. Identify all Service or agency systems that require external joint and combined interfaces with other Service or agency programs and systems.
- d. Ensure ORD interoperability KPPs along with other KPPs and critical technical and operational issues are used to develop the C4ISP and the TEMP.
- e. Ensure the PMs design includes user required external joint and combined system interfaces when modifying systems through coordination with all DOD components and allies.
- f. Participate in configuration management (CM) of interface standards.
- g. Participate in DOD efforts to influence development of non-government standards for supportability of all NSS and ITS. Implement standards in candidate systems and test those implementations for conformance with the standards.
- h. Participate in the MCEB and appropriate subpanels.
- i. Develop, in coordination with DISA (JITC), interoperability test and evaluation criteria for inclusion in acquisition documents, TEMP, and other test plan submissions. Prior to a Milestone III decision approval for all new or modified NSS and ITS, the Services and Defense agencies will ensure those systems undergo interoperability certification testing IAW these criteria. This includes any limited or prototype IOC fielding.
- j. Participate in NSS and ITS interoperability testing programs by planning, programming, budgeting, and providing resources in accordance with agreed-to schedules and test plans. Resources include the Service systems, equipment, and personnel necessary to accomplish interoperability testing. Required interoperability testing and certification will have some impact on schedule and cost of programs. These cost and schedule impacts will need to be added to POM and project cost estimates. The amount of this funding will be coordinated

8 May 2000

with the sponsor by DISA (JITC) prior to the initiation of DISA (JITC) efforts.

k. Provide direction to acquisition managers to ensure that all weapon systems that have or depend on NSS and ITS capabilities are tested for interoperability.

l. Provide guidance to all program managers to ensure that information assurance hardware and software capabilities (tools) are assessed for and meet interoperability requirements as established by the IAP.

7. Director, DISA, will:

a. Participate in the technical assessment of requirement documents and C4ISPs.

b. Exercise DISA's role as executive agent for coordinating and integrating the DOD defense information infrastructure (DII) common operating environment (COE) activities.

c. Exercise DISA's role as executive agent for coordinating and integrating the DOD ITS standards activities.

d. Manage the NSS and ITS Standards Program and administer the process to ensure that appropriate standards are available and used, including defining standards requirements and planning, prioritizing, and resourcing standards projects.

e. Provide guidance, assistance, and information on appropriate use of standards, the applicability of standards to functional areas (e.g., networking), system domains (e.g., intelligence), and program phases (e.g., use of existing standards for imminent acquisitions and use of emerging standards for long-range program planning).

f. Provide an assessment of the suitability of standards identified in MNSs, CRDs, ORDs, and C4ISPs submitted under this instruction. Standards issues that cannot be resolved will be forwarded by DISA to the SCC of the MCEB.

g. Provide systems engineering and developmental interoperability testing assistance to system developers to help ensure maximum interoperability and minimum duplication.

h. Forward interoperability system test certification results to the J-6.

8 May 2000

i. Review all available TEMPs and provide acquisition managers with recommended interoperability test and evaluation criteria for inclusion in acquisition documents and test plans.

j. Establish and conduct, in collaboration with other DOD components, an interoperability-testing program for NSS and ITS systems.

k. Certify interoperability and standards implementation or compliance to the MCEB ITP and to the developmental and operational testing organizations of DOD components.

l. Submit an annual report to the Joint Staff J-6, USD (AT&L), ASD (C3I), DOT&E, and USJFCOM containing a by-system executive summary of systems tested for interoperability with relevant information regarding certification.

m. Serve as executive agent for the MCEB ITP (reference f).

n. Coordinate with DIA in matters of networking and communications services for the DOD Intelligence Information System (DODIIS).

o. Facilitate joint interoperability across the global, theater, and tactical network boundaries.

p. Provide system engineering, planning, and program guidance to the other components to implement solutions and to facilitate joint interoperability.

q. In coordination with the National Security Agency (NSA), review, coordinate, and define tactical signals intelligence (SIGINT) standards and processes and promote security, integration, interoperability, and data sharing among systems.

r. Provide test tools and support systems in support of interoperability and standards compliance testing.

s. Designate a central office to act as a J-6 assessment tool system manager (see Appendix A, Enclosure D).

t. Designate a document assessor POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization has only one document assessor POC. The document assessor POC identifies the individual within the organization who should review a document and provides that individual with the document assessor username and

8 May 2000

password needed to access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.

u. For systems processing classified information, coordinate with the designated accrediting agent to ensure security testing considerations are addressed in interoperability testing.

v. Establish and maintain an automated process to schedule testing, monitor certification status, document IATO information, and track uncertified systems as identified.

w. In coordination with NSA, ensure that there is an adequate level of information assurance to meet the information threat identified.

8. Director, National Security Agency (NSA), will:

a. Approve all Service and USSOCOM tactical SIGINT investment programs and provide standards compliance and interoperability assessment reports to assist MDAs in production decisions.

b. Ensure DOD cryptologic programs and US Signals Intelligence Directives (USSIDs) comply with interoperability and supportability policy.

c. Ensure, in coordination with other DOD components, that requirements for cryptologic systems interoperability are satisfied through the design and development of technical, procedural, and operational interfaces between NSS and ITS systems and those intelligence systems processing foreign intelligence and foreign counterintelligence information.

d. Perform CM for cryptologic systems and jointly with DISA perform CM for the interface between cryptologic systems and the NSS and ITS systems.

e. Designate a document assessor POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization has only one document assessor POC. The document assessor POC identifies the individual in the organization who should review a document and provides that individual with the document assessor username and password needed to access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.

9. Director, National Imagery and Mapping Agency (NIMA), will:

8 May 2000

- a. Ensure that US Imagery and Geospatial System (USIGS) standards and specifications established for imagery, imagery intelligence, and geospatial information (formerly mapping, charting, and geodesy) support the interoperability of NSS and ITS via coordination with the Military Services, DISA, and the unified commands.
- b. Ensure USIGS standards and specifications incorporate imagery and geospatial information release or disclosure decisions.
- c. Ensure that commercial and nongovernmental standards used for imagery and geospatial systems and applications are open-systems based and conform to DII and DOD JTA tenets for interoperability.
- d. Designate a document assessor POC for the J-6 assessment tool (see Appendix A, Enclosure D). Each organization has only one document assessor POC. The document assessor POC identifies the individual in the organization who should review a document and provides that individual with the document assessor username and password needed to access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.

10. Director, Defense Intelligence Agency (DIA), will:

- a. Ensure that standards and specifications established for measurement and signature intelligence (MASINT) under the US MASINT System (USMS) support the interoperability of NSS and ITS systems via coordination with the Military Services.
- b. Ensure that commercial and nongovernmental standards used for MASINT systems and applications are open-systems based and conform to DII and DOD JTA tenets for interoperability.

## ENCLOSURE B

## INTEROPERABILITY KEY PERFORMANCE PARAMETERS AND TOP-LEVEL INFORMATION EXCHANGE REQUIREMENTS

1. General. This enclosure describes the development of CRD and ORD interoperability KPPs and top-level IERs based on the format and content of the integrated architecture products described in the C4ISR architecture framework (reference h).

2. Interoperability KPP. Reference a requires that CRD and ORD interoperability KPPs be derived from the set of top-level IERs. IERs characterize the information exchanges to be performed by the proposed FoS, SoS, or system. The following paragraphs discuss top-level IERs and interoperability KPPs and outline a recommended methodology to develop CRD and ORD interoperability KPPs.

3. Top-Level Interoperability IERs

a. For CRDs, top-level IERs are defined as information exchanges between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS (i.e., with other C/S/A, allied, and coalition systems).

b. For ORDs, top-level IERS are defined as those information exchanges that are external to the system (i.e., with other C/S/A, allied and coalition systems).

c. A top-level IER matrix provided in a worksheet format (i.e., Excel, LOTUS, or Quattro Pro) will be part of CRDs and ORDs when submitted. Top-level IERs identify **who** exchanges **what** information with **whom**, **why** the information is necessary, and **how** the information exchange must occur. Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission.

d. Top-level IERs and the interoperability KPP will be extracted from the ORD and used in the development of the C4ISP. Top-level IERs will be provided in the matrix format shown in Figure B-1.

e. Top-level IERs may also be imported into modeling and evaluation tools including network warfare simulation (NETWARS) and Joint C4ISR architecture planning and analysis system (JCAPS). NETWARS and JCAPS both require additional fields than those depicted in Figure B-1.

8 May 2000

f. Note that there is more detail in an ORD top-level IER matrix than in a CRD top-level IER matrix. The ORD will include all applicable top-level IER(s) identified in the CRD (if a CRD exists). If the ORD is using a time-phased, evolutionary or block requirements approach, the ORD must identify the IERs for each phase or block.

g. The top-level IER matrix must correlate with the proposed high-level operational concept graphic(s) and system interface description (discussed in paragraphs 7 and 8).

(1) Sample CRD and ORD top-level IER matrices are illustrated in Figures B-3 and B-6.

(2) In the development of the top-level IER matrix, the originator will determine if a given top-level IER is critical (top-level IER matrix field 6).

h. A CRD critical top-level IER is an information exchange that is so significant that if it does not occur the CRD mission area will be adversely impacted. IERs that must be flowed down to specific systems (ORDs) should be clearly specified in the CRD. An ORD critical top-level IER supports its associated CRD critical top-level IER, or will severely and adversely impact on a warfighter mission if not accomplished.

#### 4. Interoperability Key Performance Parameter

a. CRD interoperability KPPs, and hence the IERs that the interoperability KPPs are derived from, will be measurable. ORD interoperability KPPs, and hence the IERs that the interoperability KPPs are derived from, will be measurable and testable.

b. Top-level IERs will be used as the basis to develop interoperability KPPs. The interoperability KPP definition will include that all top-level IERs will be satisfied to the standards specified in the threshold and objective values.

c. Typically the threshold criterion for the interoperability KPP will be 100 percent accomplishment of the critical top-level IERs, and the objective criterion for the interoperability KPP will be the accomplishment of all top-level IERs.

d. If a time-phased evolutionary or block approach to stating ORD requirements is being used, the ORD should identify a separate Interoperability KPP for each phase or block.

5. CRD Interoperability KPP Development. All CRDs will have an interoperability KPP. The CRD interoperability KPP defines the level of

8 May 2000

interoperability required to be a part of the CRD FoS or SoS. The CRD interoperability KPP will use top-level IERs as the primary measure for interoperability and will outline the specific framework for CRD ORDs to follow (reference a). The following four-step methodology uses products from the C4ISR architecture framework (reference h) and is recommended to develop CRD interoperability KPPs.

Step 1. Identify **top-level** joint and combined information exchanges that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS, using a high-level operational concept graphic (OV-1) (reference h).

Step 2. Document **top-level** joint and combined IERs that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS depicted in high-level operational concept graphic (OV-1) in an operational information exchange matrix (OV-3) (reference h). Use matrix format illustrated in Figure B-1.

Step 3. Identify and label **critical** top-level IERs. A CRD critical top-level IER is an information exchange that is so significant that if it does not occur the CRD mission area will be adversely impacted. IERs that must be flowed down to specific systems (ORDs) should be clearly specified in the CRD. Critical top-level IERs will be required at threshold.

Step 4. Derive an interoperability KPP from the top-level IER matrix. A typical interoperability KPP is detailed below.

<b>Interoperability KPP</b>	<b>Threshold (T)</b>	<b>Objective (O)</b>
All top-level IERs will be satisfied to the standards specified in the threshold (T) and objective (O) values.	100% of top-level IERs designated <b>critical</b>	100% of top-level IERs

6. ORD Interoperability KPP Development. All ORDs will have an interoperability KPP.

(a) The ORD interoperability KPP defines the level of interoperability for the proposed system. The ORD interoperability KPP will be derived from the set of top-level IERs that characterize the information exchanges to be performed by the proposed system.

(b) A case may exist when an ORD does not have a set of top-level IERs. An ORD interoperability KPP that defines the level of interoperability for the proposed system may still be required.

8 May 2000

(c) ORDs that come under the umbrella of a CRD should ensure compliance with the CRD interoperability KPP (reference a).

(d) The following five-step methodology uses products from the C4ISR architecture framework (reference h) and is recommended to develop ORD interoperability KPPs.

Step 1. Identify **top-level** joint and combined external interfaces using a high-level operational concept graphic (OV-1) (reference h).

Step 2. Identify legacy, current, and future external joint and combined subsystems and interfaces that are required to exchange information using a system interface description (SV-1) (reference h).

Step 3. Document **top-level** joint and combined external IERs depicted in the OV-1 and SV-1 in an operational information exchange matrix (OV-3) (reference h). Use the matrix format illustrated in Figure B-1.

Step 4. Identify and label **critical** top-level IERs. An ORD critical top-level IER is required to support its associated CRD critical top-level IER, or will severely and adversely impact on a warfighter mission if not accomplished. Critical top-level IERs will be required at threshold. If the ORD is using a time-phased, evolutionary or block requirements approach, the ORD must identify the IERs for each phase or block.

Step 5. Derive interoperability KPP from the top-level IER matrix. A typical interoperability KPP is detailed below.

Interoperability KPP	Threshold (T)	Objective (O)
All top-level IERs will be satisfied to the standards specified in the threshold (T) and Objective (O) values ( <b>In blocks when applicable</b> ).	100% of top-level IERs designated critical	100% of top-level IERs

7. High-Level Operational Concept Graphic (OV-1). A high-level operational concept graphic will be included in all CRDs and ORDs. The focus of the graphic is to present a top-level view of the system's interoperability requirements with other current and known future systems.

a. Top-level is defined as that level of detail required to graphically illustrate how the new system exchanges information between other C/S/A, allied, and coalition systems. The graphic will show such things as missions, top-level operations, organizations, and geographical distribution

8 May 2000

of assets. The lines connecting the systems will be used to show simple connectivity and can be annotated to show what information is exchanged. Sample high-level operational concept graphics are provided in reference h and figures B-2 and B-5.

b. ORDs will include and correlate with the applicable high-level operational concept graphics identified in the CRD (if a CRD exists).

8. System Interface Description (SV-1). A system interface description is not required for CRDs, but is required for ORDs.

a. The focus of this description is to identify specific current and known future NSS and ITS subsystems and interfaces that are required to exchange information. The goal is to use established architectures for information exchange and to identify unique system information requirements that cannot be supported with current or projected architectures. The intent is to eliminate duplication and to prevent individual systems from creating stovepipe architectures.

b. The system interface description links the operational and systems architecture views by depicting the assignments of subsystems and their interfaces to the systems and described in the high-level operational concept graphics diagram. The system interface description must correlate with the provided high-level operational concept graphics. The information may be overlaid on the high-level operational concept graphics. Sample system interface descriptions are illustrated in reference h and figure B-5 in this enclosure.

9. ORD - CRD Relationship. The interrelationship between the ORD high-level operational concept graphics, system interface description, top-level IERs, KPPs, and CRD high-level operational concept graphics, top-level IERs and KPPs must be clearly identified in the ORD

.

CRD/ORD Required Fields					
1 Rationale/ UJTL Number	2 Event/Action.	3 Information Characterization.	4 Sending Node	5 Receiving Node	6 Critical
Set of joint mission tasks from the UJTL (CJCM 3500.04B) for each mission area identified in the CRD/ORD.	<b>Free Text:</b> Event or action that triggers the need for the information exchange.	<b>Pick List and Free Text:</b> The critical information characteristics that describe what information is being exchanged and how it is to be used	<b>Free Text:</b> Sending Node	<b>Free Text:</b> Receiving Node	<b>Logical Field:</b> Yes/No  The criticality assessment of the information being exchanged in relationship to the mission being performed.

ORD Required Fields (Field 10 or more are optional for CRDs/ORDs)			
7 Format	8 Timeliness	9 Classification	10 Optional
<b>Pick List and Free Text:</b> Description of data type.	<b>Numerical Field:</b> Required maximum time from node to node expressed in seconds.	<b>Pick List Field:</b> Classification of the information.	<b>Free Text:</b> As desired by the originator

Figure B-1. Top-Level IER Matrix Format

8 May 2000

10. **Top-level IER Matrix Field Definitions.** Only the first six fields are mandatory for CRDs. If data is unknown for a specific top-level IER field in the proposed ORD top-level IER matrix, annotate the field element as unknown and comment as to the anticipated boundary conditions if possible. It is expected that all ORD top-level IER field information will be available prior to a Milestone II decision. Avoid IER duplication by including an optional field identifying that the IER is bidirectional when appropriate.

- a. Field Number: 1.

Field Name: Rationale/universal joint task list number(s) **(CRD/ORD Mandatory Field)**.

Definition: Alpha-numeric field that documents the proposed system warfighting and warfighter support tasks described in the current UJTL (reference i) that this IER supports.

Field Example: TA 3.2.7 Conduct Air and Missile Defense Operations..

- b. Field Number: 2.

Field Name: Event/Action **(CRD/ORD Mandatory Field)**.

Definition: A free text field that describes the event or action that triggers the need for the information exchange.

Field Examples: Target Request; Track Update; Data Request; Track Automatic Update.

- c. Field Number: 3.

Field Name: Information characterization **(CRD/ORD Mandatory Field)**.

Definition: Pick list and free text field that describes the content of the information.

Pick List: C2, Situational Awareness, Targeting, Threat, Fire Support, Logistics, Personnel, Other specified.

Field Example: Targeting – Track update report.

- d. Field Number: 4.

Field Name: Sending node **(CRD/ORD Mandatory Field)**.

Definition: Free text field that describes the node that sends the information element.

Field Examples: JICPAC, JTF JOC, JFLCC, JAOC, JSF.

- e. Field Number: 5.

Field Name: Receiving Node **(CRD/ORD Mandatory Field)**.

Definition: Free text field that describes the node that receives the information element.

Field Examples: JICPAC, JTF JOC, JFLCC, JAOC, JSF.

8 May 2000

## f. Field Number: 6.

Field Name: Critical (**CRD/ORD Mandatory Field**).

Definition: A logical field used to characterize the importance of the information exchange. A CRD critical top-level IER is an information exchange that is so significant that if it does not occur the CRD mission area will be adversely impacted. An ORD critical top-level IER is one that is required to support its associated CRD critical top-level IER, or will severely and adversely impact on a warfighter mission if not accomplished.

NOTE: A critical IER is an interoperability KPP threshold requirement.

Field Example: Yes.

## g. Field Number: 7.

Field Name: Format (**ORD Mandatory Field**).

Definition: Pick list and free text field that describes the physical form of the information element. This is not the communications medium used to send the information.

Pick list: Audio, Text, Graphics, Imagery, Video, and Data.

Field Example: Audio - voice 5 kHz.

## h. Field Number: 8.

Field Name: Timeliness (**ORD Mandatory Field**).

Definition: Numerical field measured in seconds. It represents the time between the occurrence of the event to the time it is available to the user in seconds.

Field Example: 20 secs.

## i. Field Number: 9.

Field Name: Classification (**ORD Mandatory Field**).

Definition: Pick list field that describes the highest security classification that can be assigned to this information element.

Pick List: UNCLASSIFIED (U), CONFIDENTIAL (C), SECRET (S), TOP SECRET (TS), Sensitive Compartmentalized Information (SCI), Foreign Releasable (FR).

Field Example: C.

## j. Field Number: 10.

Field Name: Optional (**Optional CRD/ORD Field**)

Definition: Free text: Any additional field(s) the originator desires to describe an IER.

Field Examples: Position accuracy, remarks.

11. Sample CRD high-level operational concept graphic (OV-1), top-level IER matrix (OV-3), and interoperability KPP.

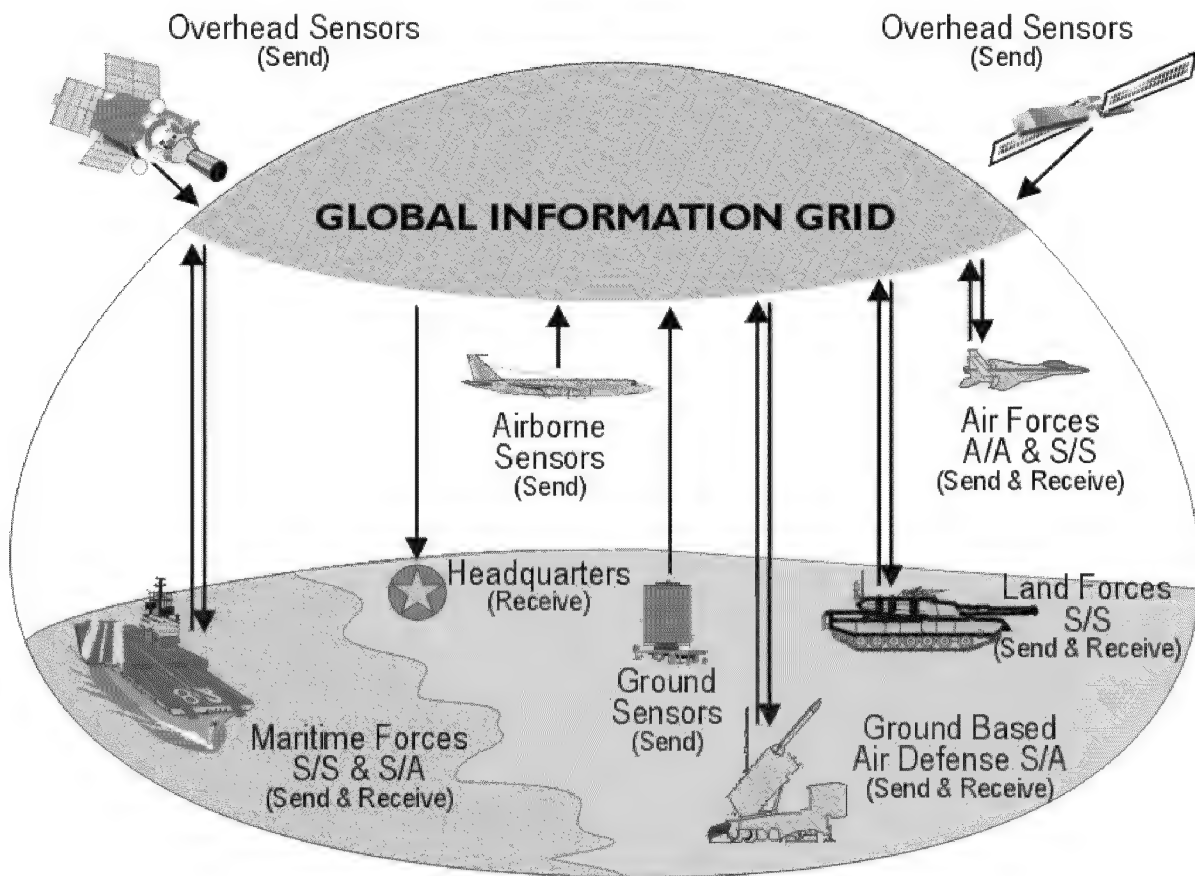


Figure B-2. Sample CRD Top-level Operational Concept View (OV-1)

NOTE: Sample is extracted from the Combat Identification (CID) CRD

NOTE: Sample IER matrix uses variables instead of actual numeric values in fields 6-8.

1	2	3	4	5	6	7	8	9
UJTL	EVENT	INFORMATION CHARACTER	SENDING NODE	RECEIVING NODE	POSITION ACCURACY	DATA INTEGRITY	TIMELINESS	CRITICAL
OP 2.2.5 Collect Target Information	Acquire info that supports the detection, ID, and location of enemy targets.	<b>Situation Awareness.</b> Target ID, Target Location, Target Track Updates	Strategic/operational/tactical sensors	Operational/tactical C2 nodes and sensors	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
OP 2.2.5 Collect Target Information	Acquire info that supports the detection, ID, and location of enemy targets.	<b>Situation Awareness.</b> Target ID, Target Location, Target Track Updates	Strategic/operational/tactical sensors	Operational/tactical C2 nodes and sensors	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
OP 3.2 Attacks Operational Targets	Attacks/engage operational targets	<b>Targeting.</b> Target ID, Target Location, Target Track Updates	Strategic/operational/tactical sensors	Operational/tactical shooters	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
OP 3.2 Attacks Operational Targets	Attacks/engage operational targets	<b>Targeting.</b> Target ID, Target Location, Target Track Updates	Strategic/operational/tactical sensors	Operational/tactical shooters	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
OP 3.2.7 Synchronize Operational Targets	Attack on single or organizational targets at decisive time and place	<b>Targeting.</b> Enemy targets, Friendly Forces, Neutrals, NCBTS, L/B, L/L, Course, Speed, Altitude, Confidence	Strategic/operational/tactical sensors	Operational/tactical shooters	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes

Figure B-3. Sample CRD Top Level IER Matrix (OV-3) (Extract from CID CRD)

NOTE: Fields 6-8 are optional fields the originator elected to use

NOTE: Sample IER matrix uses variables instead of actual numeric values in fields 6-8.

1	2	3	4	5	6	7	8	9
UJTL	EVENT	INFORMATION CHARACTER	SENDING NODE	RECEIVING NODE	POSITION ACCURACY	DATA INTEGRITY	TIMELINESS	CRITICAL
OP 3.2.7 Synchronize Operational Targets	Attack on single or organizational targets at decisive time and place	<b>Targeting.</b> Enemy targets, Friendly Forces, Neutrals, NCBTS, L/B, L/L, Course, Speed, Altitude, Confidence	Strategic/ operational/ tactical sensors	Operational/ tactical shooters	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
OP 5.1.11 Provide Positive ID of Friendly Forces within the JOA	Target ID confirmation	<b>Targeting.</b> Friendly ID, Position and Track updates, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical C2 nodes and sensors	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
OP 5.1.11 Provide Positive ID of Friendly Forces within the JOA	Target ID confirmation	<b>Targeting.</b> Friendly ID, Position and Track updates, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical C2 nodes and sensors	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
TA.3 Employ Firepower	Firepower against air, ground, and sea targets.	<b>Targeting.</b> Target ID, Target Location, Target Track Updates, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical shooters	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes

Figure B-3. Sample CRD Top Level IER Matrix (OV-3) (Extract from CID CRD) (Continued)

NOTE: Fields 6-8 are optional fields the originator elected to use

NOTE: Sample IER matrix uses variables instead of actual numeric values in fields 6-8.

1	2	3	4	5	6	7	8	9
UJTL	EVENT	INFORMATION CHARACTER	SENDING NODE	RECEIVING NODE	POSITION ACCURACY	DATA INTEGRITY	TIMELINESS	CRITICAL
TA.3 Employ Firepower	Firepower against air, ground, and sea targets.	<b>Targeting.</b> Target ID, Target Location, Target Track Updates, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical C2 nodes and sensors	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
TA 3.2 Engage Targets	Attack and engage tactical targets	<b>Targeting.</b> Target ID, Target Location, Target Track Updates, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical shooters	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
TA 3.2 Engage Targets	Attack and engage tactical targets	<b>Targeting.</b> Target ID, Target Location, Target Track Updates, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical shooters	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
TA 3.2.7 Conduct Air and Missile Defense Operations	Attack on single or organizational tactical targets at the decisive time and place	<b>Targeting.</b> Enemy targets, Friendly Forces, Neutrals, NCBTS, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical shooters	Less than AA meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
TA 3.2.7 Conduct Air and Missile Defense Operations	Attack on single or organizational tactical targets at the decisive time and place	<b>Targeting.</b> Enemy targets, Friendly Forces, Neutrals, NCBTS, L/B, L/L, Course, Speed, Altitude, Confidence	Operational/ tactical C2 nodes and sensors	Operational/ tactical shooters	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No

Figure B-3. Sample CRD Top Level IER Matrix (OV-3) (Extract from CID CRD) (Continued)

NOTE: Fields 6-8 are optional fields the originator elected to use  
B-12

NOTE: Sample IER matrix uses variables instead of actual numeric values in fields 6-8.

TA 5.1 Acquire and Communi- cate Info and Maintain Force Reporting	Reception of data from all sources	<b>Situation Awareness.</b> Track Data, ID, Position Course, Speed, Altitude, Confidence	Strategic/ operational/ tactical C2 nodes, sensors, shooters	Operational/ tactical C2 nodes	Less than meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
TA 5.1 Acquire and Communi- cate Info and Maintain Force Reporting	Reception of data from all sources	<b>Situation Awareness.</b> Track Data, ID, Position Course, Speed, Altitude, Confidence	Strategic/ operational/ tactical C2 nodes, sensors, shooters	Operational/ tactical C2 nodes	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No
TA 6.5 Provide for CID	Monitor status of friendly forces, provide positive ID of friendly forces	<b>Targeting.</b> Friendly ID, Position and Track updates, L/B, L/L, Course, Speed, Altitude, Confidence	Tactical C2 nodes and shooters	Tactical C2 nodes and shooters	Less than meters spherical error probable	Information transfer between sensor and user of BB%	Less than CC seconds	Yes
TA 6.5 Provide for CID	Monitor status of friendly forces, provide positive ID of friendly forces	<b>Targeting.</b> Friendly ID, Position and Track updates, L/B, L/L, Course, Speed, Altitude, Confidence	Tactical C2 nodes and shooters	Tactical C2 nodes and shooters	Less than XX meters spherical error probable	Information transfer between sensor and user of YY%	Less than ZZ seconds	No

Figure B-3. Sample CRD Top-Level IER Matrix (OV-3) (Extract from CID CRD) (Continued)

NOTE: Fields 6-8 are optional fields the originator elected to use

**Sample CRD Interoperability KPPs**

<b>KPP</b>	<b>Threshold</b>	<b>Objective</b>
All top-level IERs will be satisfied to the standards specified in the Threshold (T) and Objective (O) values.	100% of top-level IERs designated critical	100% of all top-level IERs

Figure B-4. Sample CRD Interoperability KPP

8 May 2000

12. Sample ORD high-level operational concept graphic (OV-1) and high-level system interface description (SV-1), Top-level IER matrix (OV-3), and interoperability KPP are illustrated below.

## ***Theater High Altitude Area Defense*** **Operational Concept Graphic/System Interface Description**

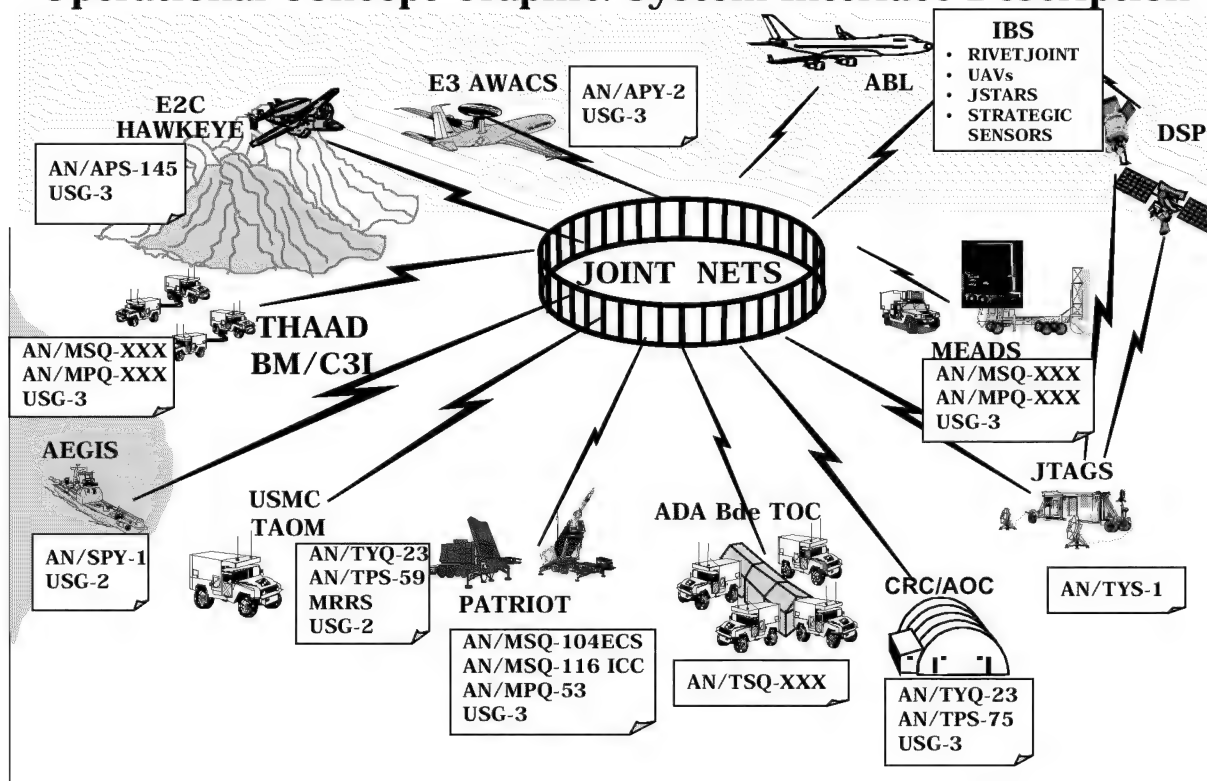


Figure B-5. Sample ORD High-level Operational Concept Graphic (OV-1) and High-level System Interface Description (SV-1)

NOTE: Sample is extracted from the THAAD ORD.

EXTRACT FROM THAAD ORD TOP-LEVEL IER MATRIX (OV-3)

1	2	3	4	5	6	7	8	9	10
Rationale UJTL #	Event	Info Char	Sending Node	Receiving Node	Crit	Format	Timeliness	Class	Remarks
OP 2.2.5 OP 2.4.2.4 OP 2.4.2.2 OP 6.1.6	TBM Launch & Detection	Targeting	IBS	THAAD	Y	Data (TADIL J)	<12 Sec	S	Sent upon launch detection to support attack operations. Both ways. Sent to THAAD initially from THAAD to support cueing to refine GIP and ELP.
OP 2.2.5 OP 2.4.2.4 OP 2.4.2.2 OP 6.1.6	TBM Launch & Detection	Targeting	CRC/AOC	THAAD	Y	Voice	<12 Sec	S	Sent upon launch detection to support attack operations. Both ways. Sent to THAAD initially, from THAAD to support cueing to refine GIP and ELP.
OP 5.3.2 OP 5.4.3	Provide ROE Update (2/Day)	Situational Awareness	PATRIOT	THAAD	N	Data (USMTF)	<2 Hrs	S	Sent to provide ROE to (Bn requirement). Both when THAAD is in task force battalion mode.
OP 2.2.4	Collect Target Information	Situational Awareness	AEGIS	THAAD	Y	Data (TADIL J)	<12 Sec	S	Acquire information that supports detection, identification, and location of enemy targets. Both ways.
OP 3.2.7	Synchronize Operational Firepower	Targeting	AEGIS	THAAD	Y	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways.
OP 5.1.1.1	Target ID Coordination	Targeting	IBS	THAAD	N	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways/THAAD Bn function.

Figure B-6. Sample ORD Top Level IER Matrix (OV-3) Extract

EXTRACT FROM THAAD ORD TOP-LEVEL IER MATRIX (OV-3)

1	2	3	4	5	6	7	8	9	10
Rationale UJTL #	Event	Info Char	Sending Node	Receiving Node	Crit	Format	Timeliness	Class	Remarks
TA 3	Firepower Against Air Targets	Targeting	JTAGS	THAAD	N	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways/THAAD Bn function.
TA 3	Firepower Against Air Targets	Targeting	PATRIOT	THAAD	N	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways/THAAD Bn function.
TA 3.2	Engage Targets	Targeting	AEGIS	THAAD	N	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways/THAAD Bn function.
TA 3.2	Engage Targets	Targeting	PATRIOT	THAAD	N	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways/THAAD Bn function.

Figure B-6. Sample ORD Top Level IER Matrix (OV-3) Extract (Continued)

EXTRACT FROM THAAD ORD TOP-LEVEL IER MATRIX (OV-3)

1 Rationale UJTL #	2 Event	3 Info Char	4 Sending Node	5 Receiving Node	6 Crit	7 Format	8 Timeliness	9 Class	10 Remarks
TA 5.1	Status/Force Reporting	Situational Awareness	ADA Bde TOC	THAAD	N	Data (USMTF)	<10 Min	S	Enemy targets, friendly forces, neutrals, noncombatants, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways.
TA 6.5	Target Combat ID Determina- tion	Targeting	JTAGS	THAAD	N	Data (TADIL J)	<12 Sec	S	Enemy targets, friendly forces, neutrals, noncombatants, deconfliction, line of bearing, ellipse, track ID, track LAT/LONG, track course, track speed, track altitude, confidence. Both ways; THAAD Bn function.
OP 5.11 OP 6.1.3	Communi- cate Operational Information	Situational Awareness	MEADS	THAAD	N	Data (USMTF)	<4 Hrs	S	Send and receive operationally significant data
OP 6.1.1	Process, Allocate Air and Missile Targets	Targeting	JTAGS	THAAD	Y	Data (TADIL J)	<12 Sec	S	Allocation of TBM targets for engagements. Both ways. ABT is a THAAD Bn function.
OP 6.1.2	Integrate Joint/Multi- national TAMD	Targeting	CRC/AOC	THAAD	Y	Data (TADIL J)	<12 Sec	S	Integration air and missile defense system with joint multinational forces at the THAAD battery. Both ways. ABT is a THAAD Bn function.
OP 6.1.2	Integrate Joint/Multi- national TAMD	Targeting	HAWKEYE	THAAD	N	Data (TADIL J)	<12 Sec	S	Integration air and missile defense system with joint multinational forces at the THAAD Bn TOC. Both ways. ABT is a THAAD Bn function.

Figure B-6. Sample ORD Top Level IER Matrix (OV-3) Extract (Continued)

EXTRACT FROM THAAD ORD TOP-LEVEL IER MATRIX (OV-3)

1 Rationale UJTL #	2 Event	3 Info Char	4 Sending Node	5 Receiving Node	6 Crit	7 Format	8 Timeliness	9 Class	10 Remarks
OP 6.1.4	Counter Enemy Air Attack	Targeting	JTAGS	THAAD	N	Data (TADIL J)	<12 Sec	S	Detect, ID and destroy attacking ABT threat. Both ways. ABT is a THAAD Bn function.
OP 6.1.5	Conduct Joint Operations Area Missile Defense	Targeting	CRC/AOC	THAAD	Y	Data (TADIL J)	<12 Sec	S	Detect and destroy enemy TBM missiles in flight. Both ways. ABT is a THAAD Bn function.
TA 1.1	Deploy/ Conduct Tactical Maneuver (8/Day)	Command & Control	CRC/AOC	THAAD	N	Data (USMTF)	<3 Hrs	S	Support positioning of forces and battlefield geometry. Both ways.
TA 5 5.2 TA 5.4 TA 5.5	Exercise Command & Control (6/Day)	Command & Control	ADA BDE TOC	THAAD	N	Data (USMTF)	<4 Hrs	S	Exercise authority and direction of supported subordinate forces. Both ways.
TA 5 5.2 TA 5.4 TA 5.5	Exercise Command & Control (6/Day)	Command & Control	PATRIOT	THAAD	N	Data (USMTF)	<4 Hrs	S	Exercise authority and direction of supported subordinate forces. Both ways.

Figure B-6. Sample ORD Top Level IER Matrix Extract (Continued)

<b>KPP</b>	<b>Threshold</b>	<b>Objective</b>
All top-level IERs will be satisfied to the standards specified in the threshold (T) and objective (O) values.	100% of top-level IERs designated critical	100% of all top-level IERs

Figure B-7. Sample ORD Interoperability KPP

ENCLOSURE C

J-6 INTEROPERABILITY AND SUPPORTABILITY CERTIFICATION  
ASSESSMENT CRITERIA

General. This enclosure describes the J-6 interoperability requirements certification assessment criteria for requirement generation documents (MNSs, CRDs, and ORDs) and the J-6 supportability certification assessment criteria for C4ISPs. Additional criteria are used by J-2 in assessing and certifying intelligence supportability.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE C

REQUIREMENT DOCUMENTS (MNSs, CRDs, ORDs)

The following tables detail interoperability requirements certification assessment criteria for requirement documents (MNSs, CRDs, ORDs). The tables are based on the MNS, CRD, and ORD formats detailed in reference a.

Table C-A-1. MNS ASSESSMENT CRITERIA

No	MNS Para	Criteria	Reference
1.	1	For AIS only: Does the MNS describe how the requirement relates to the OSD Principal Staff Assistants (PSAs), DOD Chief Information Officers, and DOD component strategic planning?	CJCSI 3170.01A, Page C-A-2
2.	2	For AIS only: Does the MNS describe the functional area or activity's current organization and operational environment and describe the shortfalls of existing capabilities?	CJCSI 3170.01A, Page C-A-2
3.	2	For AIS only: Does the MNS describe quantitative benchmarks of process performance in terms of speed, productivity, and quality of outputs where comparable processes exist in the public or private sectors?	CJCSI 3170.01A, Page C-A-2
4.	2	For AIS only: Does the MNS describe whether the function to be supported by the information technology should be performed by the organization that has identified the need or whether the function could be performed by a private sector source?	CJCSI 3170.01A, Page C-A-2
5.	2	Is the DIA-validated threat identified?	CJCSI 3170.01A, Page C-A-1
6.	2	If the DIA-validated threat involves information operations, does the MNS threat identify deficiencies placed on existing NSS and ITS by information warfare threats?	CJCSI 3170.01A, Page C-A-1
7.	5	Does this MNS include a requirement that applicable standards from the DOD JTA will be applied to ensure maximum interoperability?	CJCSI 3170.01A, Pages C-A-1,2
8.	5	Does the MNS address required NSS and ITS infrastructure support (e.g., DISN, DRSN, GCCS, GCSS, and satellite systems)?	CJCSI 3170.01A, Pages C-A-1,2
9.	5	Does the MNS address external NSS and ITS interoperability and interface requirements?	CJCSI 3170.01A, Pages C-A-1,2
10.	5	Does the MNS address releasability of the system and components to allied or coalition partners?	CJCSI 3170.01A, Pages C-A-1,2

No	MNS Para	Criteria	Reference
11.	5a	Does the MNS address the need for information releasability to allied and coalition partners?	CJCSI 3170.01A, Pages C-A-1,2
12.	5	Does the MNS address (when applicable) the electromagnetic environmental effects in which the system will be operated?	CJCSI 3170.01A, Pages C-A-1,2
13.	5	Does the MNS address NSS and ITS supportability to include logistics, manpower, personnel, training, security, and spectrum boundary constraints and certification requirements?	CJCSI 3170.01A, Pages C-A-1,2

Table C-A-2. CRD ASSESSMENT CRITERIA

No	CRD Para	Criteria	Reference
1.	2	Does the CRD summarize the nature of the threat to be countered, threat tactics, and projected future threat environment for the mission area? NOTE: Threat information should reference DIA-validated documents.	CJCSI 3170.01A, Page D-A-1
2.	3	Does the CRD describe shortcomings or absence of existing capabilities and systems to fulfill the needs of the mission area in the context of the postulated threat (e.g., weapon systems, interoperability, planning)?	CJCSI 3170, Page D-A-2
3.	3	Does the CRD describe why existing NSS and ITS operational, systems, and technical architectures cannot meet current or projected future (joint) requirements for the proposed FoS and SoS?	CJCSI 3170.01A, Page D-A-2
4.	4	Does the CRD address electromagnetic environmental effects (E3)?	CJCSI 3170.01A, Page D-A-2
5.	4	Does the CRD address releasability of the system and components to allied or coalition partners?	CJCSI 3170.01A, Page D-A-2
6.	4a	Does the CRD address the need for information releasability to allied and coalition partners?	CJCSI 3170.01A, Page D-A-2
7.	4	Does the CRD address spectrum certification and supportability?	CJCSI 3170.01A, Page D-A-2
8.	4	Is the CRD interoperability KPP measurable?	CJCSI 3170.01A, Pages D-6 and D-A-2
9.	4	Does the CRD contain a high-level operational graphic(s) (OV-1)?	CJCSI 6212.01B, Page B-2

No	CRD Para	Criteria	Reference
10.	4	Does the high-level operational graphic(s) (OV-1) present a top-level view of the FoS and SoS interoperability requirements with other current and known future systems? CRD top-level IERs are information exchanges that are between systems that make up or are external the FoS or SoS (i.e., with other C/S/A, allied, and coalition systems). The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will be used to show simple connectivity and can be annotated to show what information is exchanged.	CJCSI 6212.01B, Page B-2
11.	4	Was a top-level IER matrix (OV-3) provided in a worksheet format?	CJCSI 6212.01B, Page B-1
12.	4	Does the CRD top-level IER matrix (OV-3) contain all mandatory fields in the required format?	CJCSI 6212.01B, Page B-5
13.	4	Does the CRD top-level IER matrix (OV-3) correlate with the high-level operational graphic(s)?	CJCSI 6212.01B, Page B-1-2
14.	4	Does the CRD top-level IER matrix identify <b>who</b> exchanges <b>what</b> information with <b>whom</b> , and <b>why</b> the information is necessary? Top-level IERs identify the elements of warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint mission area.	CJCSI 6212.01B, Page B-1-2
15.	4	Does the CRD interoperability KPP definition include that all top-level IERs will be satisfied IAW their critical code to the standards specified in the threshold and objective values?	CJCSI 6212.01B, Page B-2-3
16.	4	Does the CRD interoperability KPP threshold criteria include 100 percent accomplishment of the critical top-level IERs?	CJCSI 6212.01B, Page B-2-3
17.	4	Does the CRD interoperability KPP objective criteria include 100 percent accomplishment of the critical top-level IERs, and of most or all noncritical top-level IERs?	CJCSI 6212.01B, Page B-2-3

No	CRD Para	Criteria	Reference
18.	4	Does the CRD include a requirement that applicable standards from the DOD JTA will be applied to ensure maximum interoperability?	CJCSI 3170.01A, Page D-A-2-3, CJCSI 6212.01B, Page 5
19.	4	Does the CRD address IERs between nodes of different classification?	CJCSI 3170.01A, Page D-A-2-3
20.	4	Does the CRD identify and include IA requirements?	CJCSI 3170.01A, Page D-A-2-3
21.	4	Does the CRD identify requirements, when applicable, for standardized software to ensure the needed level of interoperability?	CJCSI 3170.01A, Page D-A-2-3

Table C-A-3. ORD ASSESSMENT CRITERIA

No	ORD Para	Criteria	Reference
1.	1	Does the ORD describe the C4ISR (information exchange) operational concept?	CJCSI 3170.01A, Pages E-A-1
2.	1	For AIS ORDs without MNSs only: Does the ORD describe how the requirement relates to the OSD PSAs, DOD Chief Information Officers, and DOD component strategic planning?	CJCSI 3170.01A, Page C-A-2
3.	1	For AIS ORDs without MNSs only: Does the ORD describe the functional area or activity's current organization and operational environment and describe the shortfalls of existing capabilities?	CJCSI 3170.01A, Page C-A-2
4.	1	For AIS ORDs without MNSs only: Does the ORD describe quantitative benchmarks of process performance in terms of speed, productivity, and quality of outputs where comparable processes exist in the public or private sectors?	CJCSI 3170.01A, Page C-A-2
5.	1	For AIS ORDs without MNSs only: Does the ORD describe whether the function to be supported by the information technology should be performed by the organization that has identified the need or whether the function could be performed by a private sector source?	CJCSI 3170.01A, Page C-A-2
6.	2	Does the ORD summarize the threat to be countered and projected threat environment (NOTE: Should reference DIA- or service technical intelligence center-approved documents)?	CJCSI 3170.01A, Page E-A-1
7.	3	Does the ORD describe why existing C4ISR operational, system, and technical architecture views cannot meet the requirements for the proposed system?	CJCSI 3170.01A, Page E-A-2
8.	4	Does the ORD contain a high-level operational graphic(s) (OV-1)?	CJCSI 6212.01B, Page B-3

No	ORD Para	Criteria	Reference
9.	4	Does the high-level operational graphic(s) (OV-1) present a top-level view of the system's interoperability requirements with other current and known future systems? The focus of the graphic is to present a top-level view of the system's interoperability requirements with other current, and known future systems. Top-level is that level of detail required to graphically illustrate how the new system exchanges information between other C/S/A, allied, and coalition systems. The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will show simple connectivity and can be annotated to show what information is exchanged.	CJCSI 6212.01B, Page B-3
10.	4	Does the ORD high-level operational graphic(s) (OV-1) correlate with the associated CRD high-level operational graphic(s) (OV-1)?	CJCSI 6212.01B, Page B-3
11.	4	Does the ORD contain a system interface description (SV-1)?	CJCSI 6212.01B, Page B-3
12.	4	Does the ORD system interface description (SV-1) identify specific current and known NSS and ITS subsystems and interfaces that need to exchange information? The system interface description links together the operational and systems architecture views by depicting the assignments of subsystems and their interfaces to the systems and needlines described in the high level operational graphic diagram.	CJCSI 6212.01B, Page B-3
13.	4	Does the ORD system interface description (SV-1) correlate with the provided ORD high-level operational graphic(s) (OV-1)?	CJCSI 6212.01B, Page B-3
14.	4	Was a top-level IER matrix (OV-3) provided in a worksheet format?	CJCSI 6212.01B, Page B-2
15.	4	Does the ORD top level IER matrix (OV-3) contain all mandatory fields in the required format?	CJCSI 6212.01B, Page B-5
16.	4	Does the ORD identify the top-level IERs for the system for each mission area that the system is proposed to support (e.g., CAS, AAW, surveillance, and reconnaissance)?	CJCSI 3170.01A, Page E-A-2

No	ORD Para	Criteria	Reference
17.	4	Does the ORD top-level IER matrix (OV-3) identify <b>who</b> exchanges what information with <b>whom</b> , <b>why</b> the information is necessary, and <b>how</b> the information exchange must occur? Top-level IERs identify the elements of warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint mission area.	CJCSI 6212.01B, Page B-1
18.	4	Are all ORD top-level IERs designated critical if they are required to support an associated CRD critical top-level IER or will severely and adversely impact on a warfighter mission if not accomplished?	CJCSI 6212.01B, Page B-3
19.	4	Does the ORD top-level IER matrix (OV-3) correlate with all applicable top-level IERs in the associated CRD top-level IER matrix?	CJCSI 6212.01B, Page B-3
20.	4	Does the ORD top level IER matrix correlate with the associated ORD system interface description and ORD high-level operational graphic(s) (OV-1)?	CJCSI 6212.01B, Page B-3
21.	4	Does the ORD interoperability KPP definition include that all top-level IERs will be satisfied IAW their critical code to the standards specified in the threshold and objective values?	CJCSI 6212.01B, Page B-2-5
22.	4	Do the ORD interoperability KPP threshold criteria include 100 percent accomplishment of the critical top-level IERs?	CJCSI 6212.01B, Page B-2-5
23.	4	Do the ORD interoperability KPP objective criteria include 100 percent accomplishment of the critical top-level IERs and of most or all noncritical top-level IERs?	CJCSI 6212.01B, Page B-2-5
24.	4	Do the ORD interoperability KPP definitions include all appropriate elements of the associated CRD interoperability KPP?	CJCSI 6212.01B, Page B-3
25.	4	Are the ORD interoperability KPPs measurable and testable?	CJCSI 3170.01A, Page E-5, CJCSI 6212.01B, Page B-2
26.	4	Does the ORD address natural and man-made environmental factors (such as electromagnetic compatibility and acoustic or atmospheric propagation constraints)?	CJCSI 3170.01A, Page E-A-3

No	ORD Para	Criteria	Reference
27.	4	Does the ORD address safety issues regarding hazards of electromagnetic radiation to ordnance (HERO)?	CJCSI 3170.01A, Page E-A-3
28.	4	Does the ORD identify physical and operational information system security needs?	CJCSI 3170.01A, Page E-A-3
29.	5	Does the ORD establish information systems support objectives for initial and full operational capabilities? NOTE: Must discuss interfacing NSS and ITS at the system, subsystem, platform, and force levels. Should focus on support objectives related to NSS and ITS standardization and interoperability.	CJCSI 3170.01A, Page E-A-3
30.	5	Does the ORD describe how the system will be integrated into the NSS and ITS architecture that is forecast to exist when the system is fielded?	CJCSI 3170.01A, Page E-A-4
31.	5	Does the ORD identify data and data fusion requirements (data, voice, video), computer network support, and antijam requirements?	CJCSI 3170.01A, Page E-A-4
32.	5	Does the ORD identify unique intelligence information requirements, including intelligence interfaces, communications, and database support pertaining to the target and mission planning activities, threat data, etc?	CJCSI 3170.01A, Page E-A-4
33.	5	Does the ORD describe considerations for joint, combined, and coalition use?	CJCSI 3170.01A, Page E-A-4
34.	5	Does the ORD identify procedural and technical interfaces, communications, protocols, and standards required to be incorporated to ensure compatibility and interoperability with other Service, joint Service, NATO, and other allied and friendly nation systems?	CJCSI 3170.01A, Page E-A-4
35.	5	Does the ORD require the system to comply with applicable information technology standards contained in the current DOD JTA?	CJCSI 3170.01A, Page E-A-4

No	ORD Para	Criteria	Reference
36.	5	Does the ORD address interface requirements with the Defense Switched Network (DSN), Defense Red Switch Network (DRSN), Defense Message System (DMS), Global Command and Control System (GCCS), or the Common Operational Picture (COP)?	CJCSI 3170.01A, Page E-A-4
37.	5a	Is the requirement for an adequate level of IA required for all DOD systems that are used to enter, process, store, display, or transmit DOD information, regardless of classification or sensitivity addressed in the ORD?	CJCSI 3170.01A, Page E-4
38.	5	As part of the IA solution, does the ORD include a statement that public key infrastructure (PKI) technology will be acquired as part of this effort and will be installed and used, including in initial fielding efforts, to ensure information security over all voice, video, and data transmission? PKI implementation should also consider communications interoperability with commercial and multinational partners.	CJCSI 3170.01A, Page E-A-4
39.	5	Does the ORD address the interconnection of systems operating at different classification levels?	CJCSI 3170.01A, Page E-A-4
40.	5	Does the ORD address E3?	CJCSI 3170.01A, Page E-A-4
41.	5	Does the ORD identify a requirement for spectrum supportability?	CJCSI 3170.01A, Page E-A-4
42.	5	Does the ORD identify a requirement to obtain host-nation approval (HNA) for equipment intended for operation in an overseas area of operations?	CJCSI 3170.01A, Page E-A-4
43.	5	Does the ORD identify computer resource constraints (examples include language, computer, database, architecture, or interoperability constraints)?	CJCSI 3170.01A, Page E-A-5
44.	5	Does the ORD address all mission critical and support computer resources, including automated test equipment?	CJCSI 3170.01A, Page E-A-5
45.	5	Does the ORD identify unique user interface requirements, documentation needs, and special software certificates?	CJCSI 3170.01A, Page E-A-5
46.	5	Does the ORD identify cartographic materials, digital geospatial data, and geodetic data needed for system employment? NOTE: Where possible, NIMA standard data and DOD formats will be used.	CJCSI 3170.01A, Page E-A-6

No	ORD Para	Criteria	Reference
47.	5	Does the ORD identify requirements for radio-based communications that will be satisfied by the joint tactical radio system (JTRS) ORD?	CJCSI 6212.01B, Page E-2
48.	5	Does the ORD include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS)? If yes, does the ORD clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment after 1 Oct 2002?	CJCSI 6212.01B, Page E-2
49.	7	Does the ORD include the number of operational systems, operational and support personnel, facilities, support infrastructure and organizational, intermediate, and depot support elements that must be in place? NOTE: The impact of not meeting this objective and a window of acceptability must be addressed.	CJCSI 3170.01A, Page E-A-6
50.	7	Does the ORD adequately address the requirement for interoperability system testing and certification?	CJCSI 3170.01A, Page E-A-6

APPENDIX B TO ENCLOSURE C

C4I SUPPORT PLAN (C4ISP)

The following table details J-6 supportability assessment criteria for C4ISPs. For ACAT II and III systems, the application of these criteria will be tailored to the scope, extent, and character of the system under development. This table is based on the C4ISP format in reference j. Additional criteria are used by J-2 in assessing and certifying intelligence supportability.

Table C-B-1. C4ISP Assessment Criteria

No	C4ISP Para	Criteria	Reference
	1	Provide a high-level system description and discussion of C4ISP contents. C4ISP writers will identify program, acquisition category, and status within the acquisition cycle; state the purpose and scope of the support plan; and reference all approved (or validated) and draft documents affecting the system.	Defense Acquisition Deskbook
1.	2	Provide an overview of the specific system being developed, and include all relevant NSS and ITS support characteristics.	Defense Acquisition Deskbook
2.	2	For a weapon system, include an illustration and describe the purpose, design objectives, warhead characteristics, sensors, guidance and control navigation capabilities and limitations (if appropriate), C2 environment, and general performance envelope.	Defense Acquisition Deskbook
3.	2	For a C2 system describe system function, general bandwidth requirements, and interfaces with other NSS and ITS.	Defense Acquisition Deskbook
4.	2	For an AIS, describe the system function, its mission criticality/essentiality, interfaces with other NSS and ITS, primary databases supported, and direct or indirect impacts on warfighter missions.	Defense Acquisition Deskbook
5.	2	For all systems provide a general outline of how the system will be employed, what NSS and ITS information it will need, and how the NSS and ITS architecture should work to satisfy operational requirements.	Defense Acquisition Deskbook
6.	2	Summarize potential problem areas to highlight shortfalls in required support. Include a general description of shortfalls.	Defense Acquisition Deskbook

<b>No</b>	<b>C4ISP Para</b>	<b>Criteria</b>	<b>Reference</b>
7.	3.	Define the employment concept for the system used to derive support requirements are derived.	Defense Acquisition Deskbook
8.	3.1	Define the system's roles, missions, high-level operational concepts, operational architectures (time-phased, by mission area), types and attributes of information needed, interfaces, and information exchanges. Discuss joint guidance, doctrine, and operational procedures pertaining to the system.	Defense Acquisition Deskbook
9.	3.1	Identify and describe the system's distinct mission types and employment concepts. Identify and prioritize functions, describe the functions that are critical for specific missions, and summarize NSS and ITS requirements for each distinct mission type.	Defense Acquisition Deskbook
10.	3.2	Define mission types and the NSS and ITS support requirements associated with each type to determine NSS and ITS infrastructure requirements. This information is combined with the employment rate to derive operational NSS and ITS requirements for the system.	Defense Acquisition Deskbook
11.	3.2	Discuss the employment schema; depict the operational architecture view(s); discuss the threat and tactical considerations; describe the likely employment rate of the system; describe the time-critical events required to meet operational objectives; and address workload considerations based on the operational employment concept.	Defense Acquisition Deskbook
12.	3.2	This section will include the OV-1, OV-2, and OV-6c operational architecture view products. The OV-1 architecture view must correlate with the OV-1 product from the associated ORD.	Defense Acquisition Deskbook
13.	3.3	Provide a systems architecture view that includes a verbal and graphical description of systems and connectivity providing or supporting system functions; it is also time-phased by mission area.	Defense Acquisition Deskbook

No	C4ISP Para	Criteria	Reference
14.	3.3	For a given mission area, the systems architecture view shows how multiple systems link and integrate and may describe the capabilities and operation of particular systems within the architecture.	Defense Acquisition Deskbook
15.	3.3	The systems architecture view identifies key nodes including materiel item nodes, physical connections, association of systems to nodes, circuits, networks, warfighting platforms, and specific system and component performance parameters such as mean time between failure, maintainability, and availability.	Defense Acquisition Deskbook
16.	3.3	The systems architecture view associates physical resources and performance attributes to the operational architecture view and its requirements, consistent with standards defined in the technical architecture.	Defense Acquisition Deskbook
17.	3.3	Systems architectures should increase in detail as the acquisition progresses from milestone to milestone. At a minimum, the systems architecture should include existing or planned systems and networks that provide input to or receive output from the new system or that support primary activities related to the system to be acquired, and nodes where systems are located.	Defense Acquisition Deskbook
18.	3.3	This section will include the SV-1 system architecture view, which must correlate with the SV-1 product from the associated ORD.	Defense Acquisition Deskbook
19.	3.4	Provide a technical architecture (TV-1) that lists applicable technical standards, interfaces with systems for connectivity or interoperability and includes a discussion on interoperability and operations with coalition and allied forces. Details and supporting discussion should be included in Appendix C.	Defense Acquisition Deskbook
20.	3.4	The technical view should discuss how the standards are implemented. In most cases, the technical architecture view will identify applicable existing technical guidance, tailored as needed.	Defense Acquisition Deskbook

No	C4ISP Para	Criteria	Reference
21.	4	Document the NSS and ITS support required to satisfy the development, testing, and operational employment of the system. The focus is specifically those NSS and ITS support requirements necessary for the system or component to be successfully developed and to perform its designed function (as a consumer and as a producer of information).	Defense Acquisition Deskbook
22.	4	A strategy-to-task (STT) methodology is the preferred approach for identifying derived NSS and ITS support requirements. The STT framework establishes links between means and ends through a hierarchy of objectives. It provides an audit trail from broad objectives down to operational and tactical concepts where elements are linked together using weapons, platforms, tactics, and ITS to achieve the objectives.	Defense Acquisition Deskbook
23.	4.1	Couple each employment scheme (Section 3.1) with the corresponding employment rate (Section 3.2) and the system and technical architectures (Sections 3.3 and 3.4) to assess, characterize, and quantify the requirements placed on NSS and ITS support systems and activities.	Defense Acquisition Deskbook
24.	4.1	STT analysis will address the full range of NSS and ITS support systems and data exchange requirements, including delivery platforms; intelligence tasking, collection, processing, exploitation, analysis, production, and dissemination activities and assets; the communications infrastructure; and support staffs.	Defense Acquisition Deskbook
25.	4.1	Evaluate the qualitative and quantitative adequacy of supporting systems and activities. Include specific types and elements of information and associated characteristics and attributes such as accuracy, timeliness, volumetric estimates, and required update rates.	Defense Acquisition Deskbook

No	C4ISP Para	Criteria	Reference
26.	4.1	For systems with intelligence and geospatial needs, address the area of coverage, timeliness, security, impact, quantity, quality, assuredness, robustness, flexibility, and scalability. The level of detail used in describing the operational support requirements should be sufficient to assess supportability.	Defense Acquisition Deskbook
27.	4.1	For each external interface, the following information should be provided: Activities, organizations, or activities involved; networks or other means used to exchange information; transmission types (i.e., satellite communications (SATCOM), landline, LOS communications); communication needs (spectrum certification, supportability, host-nation authorization, and bandwidth requirements); databases and software; and critical interfaces.	Defense Acquisition Deskbook
28.	4.1	Identify the primary automated information system capabilities, computer hardware, workstations, peripherals, central processors, and routing processors. Include options such as RAM, hard disc capacity, clock speed, expansion slots, operating system, etc. State the benefits expected and reasoning for the software and hardware selected.	Defense Acquisition Deskbook
29.	4.1	Identify the types of data processed and how they will be used by the system. Identify new or updated data that may be required by the system. Identify information exchange rates.	Defense Acquisition Deskbook
30.	4.1	Specific IERs should be identified in Appendix D, including at a minimum, all top-level IERs from the associated ORD. IERs should be identified using the OV-3 operational architecture view, plus all required ORD fields specified in CJCSI 6212.01.	Defense Acquisition Deskbook
31.	4.1	Identify information security classification level required and capabilities employed. If data is encrypted, identify the type of encryption planned. Address other information assurance and critical infrastructure protection issues as appropriate.	Defense Acquisition Deskbook

No	C4ISP Para	Criteria	Reference
32.	4.2	Address required support for interoperability demonstrations and testing both within the DOD component (internal testing) and by external activities such as the JITC. This discussion should identify all information and NSS and ITS infrastructure elements necessary for realistic test and evaluation. If the testing scheme proposes simulating one or more support systems, identify the related performance parameters.	Defense Acquisition Deskbook
33.	4.3	Identify the NSS and ITS infrastructure required to support training activities prior to and after IOC. Discuss anticipated NSS and ITS support to training required for the three mutually supporting pillars of training: unit, institution, and self-development. Identify anticipated operator, crew, and net training that may be required to support joint operations. Identify anticipated use of computer-based training modules, simulations, and major exercises.	Defense Acquisition Deskbook
34.	5.0	Address shortfalls in required NSS and ITS support capabilities; shortfalls in manpower, training, or doctrine for NSS and ITS; and any other changes that must be implemented for the NSS and ITS infrastructure to support the system. Include shortfalls that limit or preclude design tradeoff studies or other analyses during program risk reduction and demonstration. Specify the impact of failure to resolve the shortfalls in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. Identify the plan and schedule to remedy each shortfall, including issues that must be resolved. If proposed for allied or coalition interoperability, identify the type of releasable encryption devices required or planned.	Defense Acquisition Deskbook
35.	5.0	Address the system's reliance on technology not currently available, other systems under development, or dependency on milestones of other programs.	Defense Acquisition Deskbook

No	C4ISP Para	Criteria	Reference
36.	5.0	If the solution to an identified shortfall lies outside the control of the DOD component, provide a recommendation identifying the organization with the responsibility and authority to address the shortfall.	Defense Acquisition Deskbook
37.	5.1	Identify potential shortfalls noted in the operational employment scheme. Focus particularly on potential support system inability to meet quantitative or qualitative requirements. Identify initial interface dependencies that remain unfulfilled, especially those beyond the program manager's control. Furthermore, note potential conflicting demands on support from other systems and activities.	Defense Acquisition Deskbook
38.	5.2	Identify potential shortfalls noted in the proposed testing and evaluation scheme. Focus particularly on potential discontinuities between the testing plan and support system and activity availability.	Defense Acquisition Deskbook
39.	5.3	Identify potential shortfalls noted in the proposed training schemes for system development as well as test and operational employment.	Defense Acquisition Deskbook
40.	Appendix A	Provide the most recent ITMRA compliance information for the program or system in this appendix.	Defense Acquisition Deskbook
41.	Appendix B	Provide a list of references that identify all related documents (with dates) used to prepare the support plan. Include all essential and any supporting products covering operational, systems, or technical architecture views such as the STAR, analysis of alternatives (AoA), COEA, MNS, ORD, TEMP, system acquisition master plan (SAMP), acquisition program baseline (APB), other C4ISPs, or any other C4ISR architectural framework products.	Defense Acquisition Deskbook

No	C4ISP Para	Criteria	Reference
42.	Appendix C	Identify information technology standards implemented by the system (technical architecture view TV-1). These standards should be based upon the JTA.	Defense Acquisition Deskbook
43.	Appendix D	The set of IERs for each external interface should be documented and described, including at a minimum, all IERs from the associated ORD. IERs should be identified using the OV-3 operational architecture view, plus all required ORD fields specified in CJCSI 6212.01.	Defense Acquisition Deskbook
44.	Appendix E	Identify documentation that indicates what interface control agreements have been made (and those that are required to be made) between dependent programs for NSS and ITS support. For example, if system A is relying on information from system B, then this interface dependency must be documented to ensure it is addressed. At a minimum, these dependencies should be identified in the C4ISPs for both systems A and B.	Defense Acquisition Deskbook

(INTENTIONALLY BLANK)

## ENCLOSURE D

### PROCEDURES

1. General. The Joint Staff J-6 performs interoperability requirements certification (MNSs, CRDs, ORDs); supportability certification (C4ISPs); and interoperability system validation.

a. J-6 Interoperability Requirements Certification. This certification occurs prior to each acquisition milestone (0, I, II, III).

(1) The J-6 certifies MNSs, CRDs, and ORDs regardless of ACAT level for conformance with joint NSS and ITS policy and doctrine and interoperability standards. The J-6 also certifies the interoperability KPP derived from a set of top-level IERs.

(2) As part of the review process, J-6 requests assessments from the Services, DISA, and DOD agencies. CINCs are required to review and comment on ACAT I/IA and JROC special interest requirements documents during the J-8 (JROC) formal review. CINCs are provided the opportunity to review and comment on ACAT II and below documents during the J-6 interoperability requirements certification process.

(3) USJFCOM, as the joint force integrator, will review and confirm the sufficiency of interoperability KPPs and IER matrices for all CRDs and ORDs regardless of ACAT. The J-6 forwards interoperability certification to the JROC for ACAT I/IA and JROC special interest programs or to the sponsoring DOD component for ACAT II and below programs.

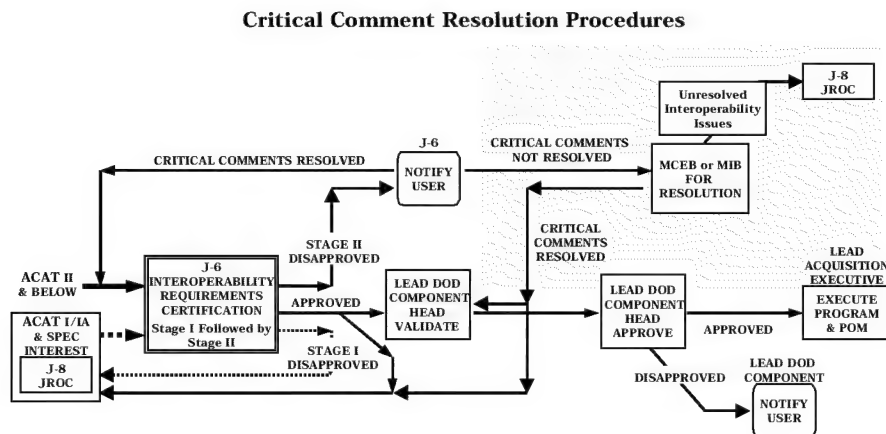


Figure D-1

8 May 2000

(4) J-6 will forward unresolved interoperability issues to the MCEB or MIB for resolution. The MCEB or MIB will return resolved interoperability issues to the lead DOD component to complete JROC approval process. The MCEB and MIB will ensure that unresolved issues resulting from interoperability assessments are presented to the JROC for resolution (see Figure D-1).

b. Supportability Certification. The J-6 certifies to ASD (C3I) that C4ISPs, regardless of ACAT, adequately address NSS and ITS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems.

(1) As part of the review process, J-6 requests supportability assessments from DISA and DOD agencies. CINCs are provided the opportunity to review and comment on documents, regardless of ACAT, during the J-6 supportability certification process.

(2) J-6 conducts a supportability certification for C4ISPs prior to Milestone I, II, and III for submission to ASD (C3I) as part of the C4ISP review process.

(3) In a related but separate process, J-2 provides certification of intelligence supportability.

c. J-6 Interoperability System Validation. The J-6 validation is intended to provide total life-cycle oversight of warfighter interoperability requirements. The J-6 validates that the interoperability KPP derived from the set of top-level IERs approved in the CRD (if applicable), ORD, and C4ISP was adequately tested and testing results certified during the DISA (JITC) interoperability system test certification. Fifteen days after receipt of the DISA (JITC) interoperability system test certification memorandum, the J-6 will issue an interoperability system validation memorandum to the respective Services, agencies, and developmental and operational testing organizations.

2. Assessment Procedure Overview. Documents submitted by C/S/As will be evaluated early in the life cycle of a system and at all acquisition milestones to help the developer ensure that a system or program will successfully achieve system test certification and eventual fielding.

a. During the interoperability certification process, J-6 requests technical assessments from DISA, Services, and other DOD agencies.

8 May 2000

b. USJFCOM, as the joint force integrator, will review and confirm the sufficiency of interoperability KPPs and IER matrices for all CRDs and ORDs regardless of ACAT.

c. CINCs are required to review and comment on ACAT I/IA and JROC special interest requirements documents during the J-8 (JROC) formal review. CINCs are provided the opportunity to review and provide warfighter comments during the J-6 interoperability requirements certification process.

d. J-6 uses a DISA-managed electronic tool, the J-6 assessment tool, to enhance the staffing, coordination, and compilation of assessment comments (Figure D-2). Additional information on the J-6 assessment tool is explained in Appendix A to this enclosure.

(1) J-6 interoperability certifications of MNSs, ORDs, and CRDs are conducted in three distinct stages. J-6 supportability certifications of C4ISPs are conducted in two stages. ASD (C3I) is responsible for Stage III for C4ISPs.

(a) Stage I is the draft assessment for all ACATs of a MNS, ORD, CRD, or C4ISP.

(b) Stage II is the final assessment and certification of the same documents.

(c) Stage III is the posting of the JROC- or MDA-approved MNS, CRD, and ORD. Approved documents are filed in the J-6 assessment tool with the J-6 certification letter.

e. The suspense for completing a Stage I MNS, ORD, CRD, or C4ISP certification is 35 sequential days from electronic submission date to the J-6 assessment tool.

f. The Stage II suspense is 21 sequential days.

g. The Stage III suspense is 15 sequential days after JROC or MDA approval.

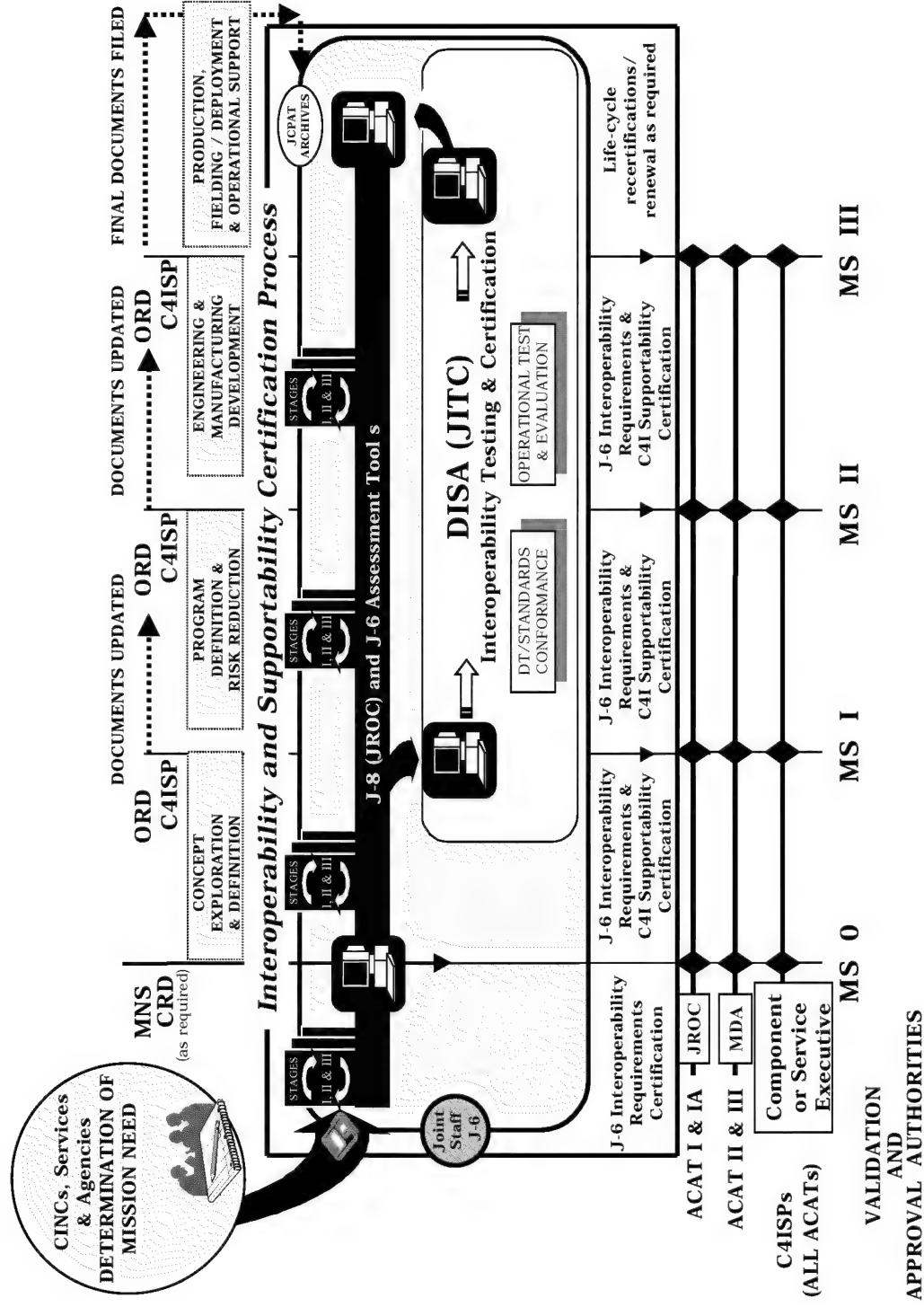


Figure D-2. Requirements and Acquisition Interface

8 May 2000

h. J-6 interoperability and J-6 supportability certification approval authority for each stage is detailed in Table D-1.

DOCUMENT	STAGE	J-6 CERTIFICATION APPROVAL AUTHORITY
MNSs/ORDs ACAT I/IA	I	06
	II	FLAG
	III	J-8 JROC*
CRDs	I	06
	II	FLAG
	III	J-8 JROC*
MNS/ORD ACAT II & III	I	06
	II	06
	III	C/S/A*
C4ISP ACAT I/IA	I	06
	II	FLAG
C4ISP ACAT II-III	I	06
	II	06

\*NOTE: Posting Approval Authority

Table D-1. J-6 Certification Approval Authority

i. All DOD requirements originators and assessors (C/S/As) will use the J-6 assessment tool to submit documents and assessor comments to J-6 on all MNSs, ORDs, CRDs, and C4ISPs.

j. During Stages I and II, assessor comments will be categorized as detailed below.

CRITICAL. A critical comment indicates nonconcurrence with the document until the comment is satisfactorily resolved.

8 May 2000

SUBSTANTIVE. A substantive comment is provided because a section in the document appears to be or is potentially unnecessary, incorrect, misleading, confusing, or inconsistent with other sections. A substantive comment not resolved in Stage I could result in a critical Stage II comment. Additionally, multiple substantive comments could also result in a critical comment.

ADMINISTRATIVE. An administrative comment corrects what appears to be a typographical, format, or grammatical error.

k. Formal comments will indicate the page and paragraph numbers from the document and provide a rewrite recommendation and a rationale.

l. Document submitters may contact POCs identified in J-6 certification memorandum to discuss critical comments. Resolved critical comments must be incorporated in Stage II document. Stage I critical comments will be resolved during Stage II. Unresolved Stage II critical comments will be forwarded by J-6 to the MCEB or MIB for resolution.

## APPENDIX A TO ENCLOSURE D

### J-6 ASSESSMENT TOOL

1. General. The J-6 assessment tool is the primary software tool used to manage the assessment and storage of MNSs, CRDs, ORDs, and C4ISPs. The tool is part of the joint C4I program assessment tool (JCPAT) that DISA operates and maintains for the Joint Staff and ASD (C3I). Other JCPAT tools include the J-8 JROC assessment tool and ASD (C3I) C4ISP tool. The J-6 assessment tool provides a collaborative work area, automated mail and distribution function, and an archival capability. An extensive reference library of requirement documents is available for C/S/As use (See Figures D-A-1 and D-A-2).

2. J-6 Assessment Tool Access.

a. The J-6 classified assessment tool may be accessed via the SIPRNET at <http://jcpat.ncr.disa.smil.mil>; unclassified portions may be accessed via the NIPRNET at <http://iap.ncr.disa.mil>.

b. A user ID and password are required to use the tool and may be requested from J-6I.

3. J-6 Assessment Tool Functionality. The J-6 assessment tool consolidates and formats assessment comments from C/S/As. J-6 reviews the consolidated documents, then in turn completes an interoperability requirements or supportability certification. The J-6 assessment tools enhance the on-line electronic staffing of assessment documents. Automated E-mails are sent to assessor organization POCs (see Table D-A-1) to provide notification of new document availability on line. Each assessor group has distinct privileges. User responsibilities must be considered when groups are configured.

4. J-6 Assessment Tool Group Responsibilities. J-6 assessment tool groups and responsibilities are detailed below.

a. Joint Staff/J-6. Executive agent. Uses the J-6 assessment tool to automate the NSS and ITS assessment process. Using the J-6 assessment tool, receives new electronic requirements and C4ISP documents, distributes them-with joint staff transmittal document, electronically collects comments, and prepares and posts the interoperability certification memorandum.

b. Document Submitter Group. An organization (C/S/A) that electronically submits an ACAT II or III requirements document to the J-6 assessment tool for J-6 interoperability certification.

(1) All ACAT I/IA requirements documents are received directly from the J-8 JROC assessment tool.

(2) All C4ISP documents are received directly from the ASD (C3I) C4ISP tool.

c. Document Assessor Group. A C/S/A POC responsible for managing NSS and ITS assessments via the J-6 assessment tool. The document assessor POC

(1) Regularly accesses the J-6 assessment tool and accounting for and responding to all J-6 taskings.

(2) Coordinates the assessment of assigned requirements and C4ISP documents within his or her C/S/A.

(3) Returns the C/S/A's consolidated comments to J-6 electronically via the J-6 assessment tool.

(4) Identifies the individual within the organization responsible for reviewing a document and provides that individual document assessor username and password needed to access the J-6 assessment tool. The document assessor username and password are obtained from J-6I.

NOTE: Each C/S/A has only one document assessor POC. Only the C/S/A document assessor POC can send the consolidated assessment comments back to the J-6 assessment tool.

d. Table D-A-1 details J-6 assessment tool groups.

Table D-A-1.J-6 Assessment Tool Groups

<b>ORGANIZATION</b>	<b>LOCATION</b>	<b>J-6 ASSESSMENT TOOL ROLE</b>	<b>DOCUMENTS</b>
Joint Staff J-6	Pentagon	J-6 Assessment Tool Executive Agent	MNSs, ORDs, CRDs, C4ISPs
ASD (C3I)	Crystal Mall III, Alexandria, VA	Document Assessor	MNS, CRD, ORD
Joint Staff J-2	Pentagon	Document Assessor	MNSs, ORDs, CRDs
USA, TRADOC	Ft Monroe, VA	Document Submitter/Assessor	MNSs, ORDs, CRDs
USN, CNO	Pentagon	Document Submitter/Assessor	MNSs, ORDs, CRDs
USAF, XORD	Pentagon	Document Submitter/Assessor	MNSs, ORDs, CRDs
USMC	Quantico, VA	Document Submitter/Assessor	MNSs, ORDs, CRDs
USCENTCOM	MacDill AFB, FL	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USEUCOM	Vaihingen, Germany	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USJFCOM	Norfolk, VA	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USPACOM	Camp H. M. Smith, HI	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USSOUTHCOM	Miami, FL.	Document Submitter/ Assessor	MNSs, CRDs, ORDs, C4ISPs
USSPACECOM	Peterson AFB, CO	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USSOCOM	MacDill AFB, FL	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USSTRATCOM	Offutt AFB, NE	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
USTRANSCOM	Scott AFB, IL	Document Submitter/Assessor	MNSs, CRDs, ORDs, C4ISPs
DISA	Arlington, VA	Document Assessor	MNSs, ORDs, CRDs, C4ISPs
DISA (JITC)	Ft. Huachuca, AZ	Document Assessor	MNSs, ORDs, CRDs, C4ISPs, System Test Certification results
DISA (JSC)	Annapolis, MD	Document Assessor	MNSs, ORDs, CRDs, C4ISPs

8 May 2000

ORGANIZATION	LOCATION	J-6 ASSESSMENT TOOL ROLE	DOCUMENTS
NSA	Ft. Meade, MD	Document Submitter/Assessor	MNSs, CRDs, ORDs
NIMA	Reston, VA	Document Submitter/ Assessor	MNSs, ORDs, CRDs
DIA	Pentagon	Document Submitter/ Assessor	MNSs, ORDs, CRDs

## 5. Detailed J-6 Certification Procedures

a. Interoperability Requirements Certification MNSs, CRDs, and ORDs. The process is divided into three stages. Each stage is described step-by-step in the following paragraphs.

(1) Stage I – Draft Assessment. The assessment process is depicted in Figure D-A-1. Thirty-five sequential days are allocated for a Stage I assessment after a document submission on the J-6 assessment tool. The J-6 assessment tool archives is available for C/S/As to use in developing MNSs and ORDs and to search for status of documents.

### (a) ACAT I/IA and JROC Special Interest Requirements Documents

1 Originating C/S/As submit draft ACAT I/IA MNSs, CRDs, and ORDs electronically to the Joint Staff (J-8) JROC Secretariat via the J-8 JROC assessment tool in JCPAT.

2 Once tasked by the J-8, the J-6 electronically distributes the documents via the J-6 assessment tool for review and comment.

3 For ACAT I/IA and JROC special interest requirements documents, J-8 tasks the CINCs to review and comment.

4 J-6 uses the J-6 assessment tool to consolidate all assessment comments into the J-6 certification memorandum. The J-6 certification memorandum is forwarded to the J-8. The process is detailed in the steps following paragraph (b) below.

(b) ACAT II and Below Requirements Documents. C/S/As submit ACAT II and below MNSs, CRDs, and ORDs electronically to the J-6 via the J-6 assessment tool for certification. J-6 requests technical assessments from DISA, Services, and DOD agencies. CINCs are provided the opportunity to review and comment on ACAT II and below documents. J-6 uses the J-6 assessment tool to consolidate all assessment comments into the J-6 certification memorandum. The J-6

Step 1. Originating C/S/As submit MNS, CRD, and ORD electronically to the J-8 JROC or J-6 assessment tools (document submission screens as depicted in Figure D-A-1).

Step 3. J-6 assessment tool notifies all assessor group POCs via automated E-mail that a new requirements document is available for assessment on-line. Assessors review and submit comments to the J-6 assessment tool electronically.

Step 5. J-6 sends interoperability requirements certification memorandum to C/S/A or J-8 RAD for ACAT I/IA via J-6 assessment tool.



Appendix A  
Enclosure D

8 May 2000

The Stage II process mirrors the Stage I process. Twenty-one sequential days are allocated for a Stage II assessment after a document submission. The Stage II assessment and certification process is described in the following steps.

Step 1. Same as Stage I, Step 1. Originating C/S/As submit MNS, CRD, and ORD electronically via the J-6 assessment tool as depicted in Figure D-A-1. Critical Stage I comments resolved off-line must be incorporated in the Stage II submitted document.

Step 2. Same as Stage I, Step 2. J-6 (or J-8 RAD for ACAT I/IA) creates tasking memorandum and suspense date.

Step 3. Same as Stage I, Step 3. J-6 assessment tool notifies all assessor group POCs via automated E-mail that a new requirements document is available for assessment on-line. Assessors review and submit comments to the J-6 assessment tool electronically.

Step 4. Same as Stage I, Step 4. J-6 consolidates comments via J-6 assessment tool. Unresolved Stage II critical comments will be forwarded by J-6 to the MCEB or MIB for resolution.

Step 5. Same as Stage I, Step 5. J-6 sends interoperability requirements certification memorandum to C/S/A or J-8 RAD for ACAT I/IA via J-6 assessment tool.

(d) Stage III – Posting of Final Document. Stage III is the posting of the ACAT II or III MDA approved MNS, CRD, or ORD. The Stage III suspense is 15 sequential days after JROC or MDA approval. Approved documents are filed in the J-6 assessment tool with the J-6 certification letter. J-8 RAD electronically files JROC approved ACAT I/IA or JROC special interest documents to the J-8 JROC assessment tool.

b. J-6 Supportability Certification of C4I Support Plans (C4ISPs). C4ISPs are an acquisition document, and ASD (C3I) is the executive agent. J-6 reviews, comments, and certifies C4ISPs to ASD (C3I). The J-6 review process is similar to the interoperability requirements certification process described above.

(1) Stage I – Draft Assessment. The J-6 process is identical to the Stage I and II five-step processes detailed above for J-6 interoperability certification of requirements documents. The only difference is that C4ISPs are submitted on line via the ASD (C3I) C4I support plan tool on the JCPAT. ASD (C3I) tasks J-6 to perform a supportability certification as part of the overall C4ISP review process. Thirty-five sequential days

are allocated for a Stage I assessment after a document submission on the J-6 assessment tool. The process is detailed in the following steps and Figure D-A-2.

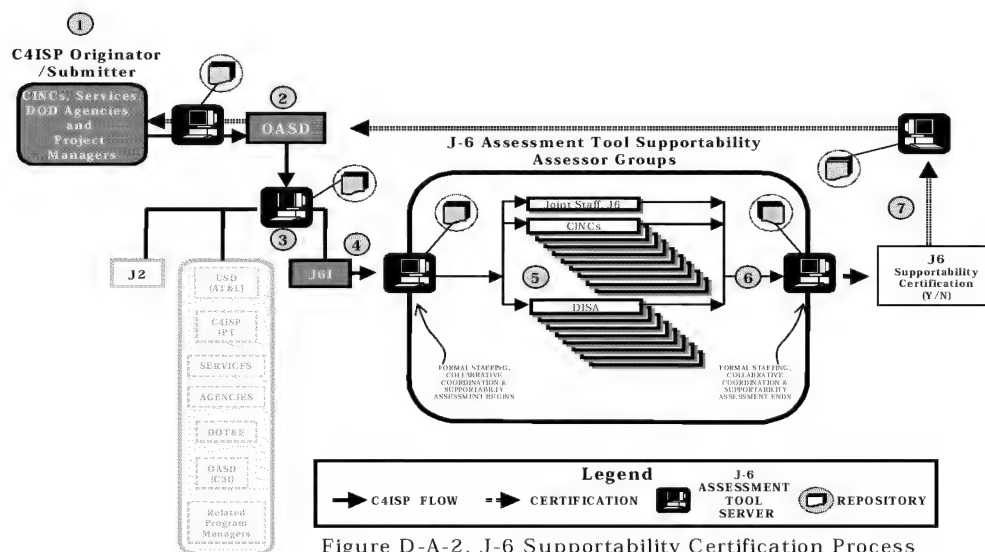
Step 1. Originating Service, agency ,or program manager submits the C4ISP electronically via the ASD (C3I) C4I support plan tool document submission screen.

Step 2. ASD (C3I) creates tasking memorandum and suspense date.

Step 3. ASD (C3I) C4I support plan tool notifies all assessor group POCs (to include J-6) via automated E-mail that a new C4ISP document is available for assessment on-line.

Step 4. J-6 creates tasking memorandum and suspense date.

Step 5. J-6, via J-6 assessment tool, notifies DISA, DISA (JTIC), DISA (JSC), DISA (CFITS), and CINCs via automated E-mail that a new C4ISP document is available for assessment on-line. CINCs are provided the opportunity to review and provide warfighter comments. Assessors review and submit comments to the J-6 assessment tool electronically.



Step 6. J-6 consolidates comments via J-6 assessment tool. Originating assessors may contact POCs identified in the J-6 supportability certification memorandum to discuss critical comments. Resolved critical stage I comments must be incorporated in Stage II submitted document. Stage I critical comments will be resolved during

8 May 2000

Stage II. J-6 will forward unresolved Stage II critical comments to ASD (C3I) for resolution.

Step 7. J-6 sends a supportability certification memorandum to ASD (C3I), originating Service, agency, or program manager via ASD (C3I) C4I support plan tool.

(2) Stage II – Final Assessment and Certification. The objective of this step is to obtain a J-6 supportability certification. The Stage II process mirrors the Stage I process. Twenty-one sequential days are allocated for a Stage II assessment after a document submission. The Stage II assessment and certification process is described in the following steps:

Step 1. Same as Stage I, Step 1. Originating Service, agency or program manager submits the C4ISP on-line via the ASD (C3I) C4ISP support plan tool document submission screen. Resolved critical stage I comments must be incorporated in the Stage II submitted document.

Step 2. Same as Stage I, Step 2. ASD (C3I) creates tasking memorandum and suspense date.

Step 3. Same as Stage I, Step 3. ASD (C3I) C4I support plan tool notifies all assessor group POCs (to include J-6) via automated E-mail that a new C4ISP document is available for assessment on-line.

Step 4. Same as Stage I, Step 4. J-6 creates tasking memorandum and suspense date.

Step 5. Same as Stage I, Step 5. J-6, via J-6 assessment tool module, notifies DISA, DISA (JTIC), (JSC), (CFITS), and CINCs via E-mail that a new C4ISP document is available for assessment. CINCs are provided the opportunity to review and provide warfighter comments. Assessors review and submit comments to J-6 assessment tool on-line.

Step 6. Same as Stage I, Step 6. J-6 consolidates comments via J-6 assessment tool. Originating assessors may contact POCs identified in the J-6 supportability certification memorandum to discuss critical comments off-line. Critical stage I comments resolved off-line must be incorporated in the Stage II submitted document. Stage I critical comments will be resolved during Stage II. J-6 will forward unresolved Stage II critical comments to ASD (C3I) for resolution.

Step 7. Same as Stage I, Step 7. J-6 sends a supportability certification memorandum to ASD (C3I), originating Service, agency, or program manager via ASD (C3I) C4I support plan tool.

APPENDIX B TO ENCLOSURE D

INTEROPERABILITY TESTING AND TEST CERTIFICATION PROCESS

1. General. All NSS and ITS, regardless of ACAT, must be tested and testing results certified by DISA (JITC). Testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early user tests) whenever possible to conserve resources.

a. DISA (JITC) must be involved during the planning and execution of interoperability test certification at each program fielding milestone and recertification. DISA (JITC), in coordination with the C/S/As, will ensure that the required data elements for interoperability system test certification are collected and validated.

b. Tests will be conducted using operational facilities and the Services' or DISA test beds during developmental testing and operational testing (DT/OT) periods.

(1) Based on such testing, DISA (JITC) will conduct an independent analysis of the data and certify that interoperability KPP have been met and the system meets criteria for joint, combined, or coalition use.

(2) This certification will include an assessment of individual IERs and overall system interoperability performance.

b. The intent is to ensure that no new system or system under modification will enter production and gain IOC without certification, and that interoperability deficiencies are detected sufficiently early in the milestone approval process to ensure interoperability standards are met by IOC.

c. For commercial-off-the-shelf (COTS) systems and software not requiring formal acquisition review, Service-sponsored interoperability testing and DISA (JITC) certification will be conducted prior to IOC.

d. The MCEB IPTP resolves issues concerning joint testing and interoperability system test certification.

e. Intelligence interoperability issues will be referred to the MIB.

f. The MCEB IPTP may grant a temporary waiver from interoperability system test certification – an IATO – in special situations based on justifiable circumstances and impacts.

2. Interoperability Test Certification Process. Interoperability test certification begins during requirements development, and continues until a system is no longer in the inventory. Figure D-B-1 depicts the role of various elements of the interoperability test certification process. DISA (JITC) can also tailor the test programs of nontraditional acquisitions to meet interoperability test certification requirements.

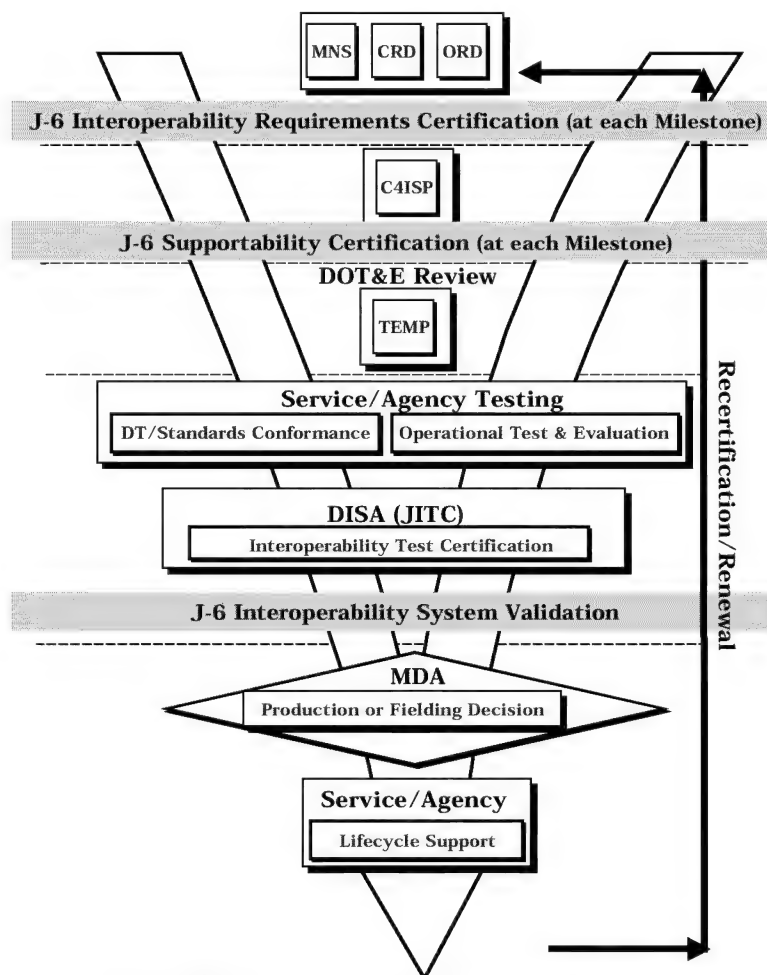


Figure D-B-1. Interoperability System Test Certification Process

a. System Tracking Program. Information from the J-6 interoperability requirements certification is used as an input to the DISA (JITC) System Tracking Program (STP). The STP is used to schedule and track tests and resources required for interoperability system test certification. Program managers and organizations with a requirement for interoperability system test certification or test support should contact the DISA (JITC) for assistance. Initial STP entries should be made as early in the acquisition process as possible. The STP program uses milestones to trigger notification to appropriate parties of upcoming certification activities or missed events.

b. Interoperability Test Certification. Interoperability test certification ensures a system meets user interoperability requirements.

(1) DISA (JITC) works with the system proponent and develops an interoperability certification evaluation plan (ICEP) that makes the most efficient use of resources. This ICEP uses existing data and other testing results to provide the requisite information. The ICEP outlines how the system will be tested against the requirements in the ORD, C4ISP, and TEMP. The testing is conducted during DT&E, OT&E, and various joint exercises and deployments. Whenever possible, testing is conducted in Service or DISA facilities during DT or OT periods.

(2) DISA (JITC) evaluates interoperability in the most operational realistic environment possible.

(3) When DISA (JITC) is not the interoperability testing organization, interoperability test plans, analysis, and reports will be coordinated with, and approved by, DISA (JITC) to ensure sufficient information is available to allow a certification decision.

(3) Developmental Testing (DT). DISA (JITC) will work with the program management office through the C/S/A to determine if the system conforms to applicable standards. Standards conformance testing of a system to a profile is performed under the direction of the PM, usually by one of their contractors or the DISA (JITC).

(2) Operational Testing (OT). DISA (JITC) works with the program management office through the C/S/A to ensure joint interoperability testing requirements are met and that the data collected is adequate for evaluating interoperability issues. The ICEP is normally completed during OT. DISA (JITC) reports any interoperability problems in the use or deployment of the system under test.

c. Production and Fielding Decision.

(1) DISA (JITC) provides the program manager, user command, DOT&E, and J-6 an interoperability test certification memorandum that can be used as input into the production and fielding decision. Interoperability for each system will be based on testing the interoperability KPP.

(2) The interoperability KPP is derived from the set of top-level external joint and combined IERs that characterize the information exchanges to be performed by the proposed system.

8 May 2000

(3) All ORD threshold interoperability KPPs will be used to develop the TEMP measures of effectiveness.

(4) DISA (JITC) interoperability test certification will include an evaluation as to whether the system is ready for joint, combined, and coalition use.

d. Life-cycle Support

(1) DISA (JITC) assesses systems during exercises and operational use to determine if changes to joint NSS and ITS architecture, standards, operational concepts, or procedures have affected interoperability.

(2) In addition, DISA (JITC) documents the employment of NSS and ITS systems that deviate from the MNS, CRDs, and ORDs.

(3) Identified deviations, deficiencies, and uncertified (never certified or expired certification) systems are tracked and reported to the Joint Staff J-6 for appropriate action.

3. Summary. Interoperability test certification of joint, combined, and coalition interoperability is a complex process requiring the full cooperation of the requirements and acquisition community. The goal is to ensure interoperability in the intended operational environment. This includes established interoperability characteristics, as well as the risks relating to the use of untested configurations. The interoperability test certification process ensures the warfighter has an effective and integrated array of systems and networks that will meet all mission needs.

ENCLOSURE E

NSS AND ITS SYSTEM SPECIFIC POLICIES

1. Purpose. Identify NSS and ITS related policies that impact J-6 certifications.
2. Policies. Requirements documents (MNSs, CRDs, and ORDs) need to address the NSS and ITS related policies detailed below.
  - a. Electromagnetic Environmental Effects and Spectrum Management Policy
    - (1) All NSS and ITS systems must be mutually compatible with other systems in the electromagnetic environment and not be degraded below operational performance requirements due to electromagnetic environmental effects (reference l).
    - (2) All NSS and ITS systems must comply with reference k.
    - (3) All proposed NSS and ITS systems that include spectrum-dependent hardware must document spectrum certification of the hardware (reference k).
    - (4) Commercial and nondevelopmental items must also comply with the aforementioned policy statements (reference k and l).
  - b. Host-nation Approval (HNA). To ensure compatibility as well as interoperability, all NSS and ITS and equipment that are intended for operation in host nations will require HNA coordinated by the MCEB and the appropriate CINCs prior to use. Hardware that does not have HNA can be confiscated or denied operation by host nations (reference l).
  - c. Joint Tactical Radio System (JTRS). All future requirements for radio-based communications will be satisfied by inclusion in the JTRS ORD unless a waiver is granted by ASD (C3I). No preplanned product improvements or in-service modifications should be undertaken that duplicate JTRS without prior approval and waiver from ASD (C3I) (reference m).
  - d. Selective Availability Anti-Spoofing Module (SAASM). All systems that include NAVSTAR GPS and PPS will develop and procure only SAASM-based equipment after 1 October 2002 (reference n).
  - e. Information Assurance. NSS and ITS, including commercial and nondevelopmental items, must comply with applicable DOD IA policies

8 May 2000

and regulations. This includes implementation of public key (PK) when required to ensure information security over all voice, video, and data transmission. Interconnection of systems operating at different classification levels will be accomplished by processes (e.g., SECRET and Below Interoperability (SABI) and TOP SECRET and Below Interoperability (TSABI)) that have been approved by the DOD chief information officer (CIO). IA will be an integral part of all interoperability efforts thus allowing appropriate security measures to protect mission data and system resources from all known threats (reference o, p, and q).

ENCLOSURE F

REFERENCES

- a. CJCSI 3170.01A, 10 August 1999, "Requirements Generation System"
- b. DOD Regulation 5000.2R, 15 March 1996, "Mandatory Procedures for Major Defense Acquisition Program (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs."
- c. DOD Directive 5000.1, 15 March 1996, "Defense Acquisition"
- d. DOD Directive 4630.5, 12 November 1992, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems"
- e. DOD Instruction 4630.8, 18 November 1992, "Procedures for Compatibility, Interoperability, C4I Supportability of Command, Control, Communications, and Intelligence Systems"
- f. MCEB Pub 1, 1 December 1998, "Organization, Mission and Function Manual"
- g. DOD Joint Technical Architecture Version 3.0, 15 November 1999
- h. C4ISR Architecture Framework, Version 2.0, 18 December 1997
- i. CJCSM 3500.04B, 1 October 1999, "Universal Joint Task List"
- j. DOD Electronic Desk Reference Set, December 1999, "Defense Acquisition Deskbook"
- k. DOD Directive 4650.1, 24 June 1987, "Management and Use of the Radio Frequency Spectrum"
- l. DOD Directive 3222.3, 20 August 1990, "DOD Joint Electromagnetic Environmental Effects Program and JSC Charter"
- m. ASD(C3I) memorandum, 28 August 1998, "Radio Acquisitions"
- n. CJCSI 6140.01, 15 November 1998, "NAVSTAR Global Positioning System Selective Availability Anti-Spoofing Module Requirements"
- o. DepSecDef memorandum, 7 December 1998, "Department of Defense (DOD) Public Key Infrastructure (PKI)"

8 May 2000

p. ASD (C3I) memorandum, 20 March 1997, "Secret and Below Interoperability (SABI)"

q. DOD Instruction 5200.4, 30 December 1997, "DOD Information Technology Security Certification and Accreditation (C&A) Process"

## GLOSSARY

### PART I--ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition Category
ABT	air-breathing targets
ADA	air defense artillery
AIS	Automated Information System
AoA	Analysis of Alternatives
AOC	air operations center
APB	Acquisition Program Baseline
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
AWACS	Airborne Warning and Control System
Bde	Brigade
Bn	Battalion
C2	command and control
C3I	command, control, communications, and intelligence
C4I	command, control, communications, computers, and intelligence
C4ISP	command, control, communications, computers, and intelligence support plan
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAE	component acquisition executive
CD-ROM	Compact Disk-Read Only Memory
CFITS	Center For Information Technology Standards
CID	combat identification
CINCs	commanders of combatant commands
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CM	configuration management
CNO	Chief of Naval Operations
COE	common operational environment
COEA	cost and operational effectiveness analysis
COP	common operational picture
COTS	commercial-off-the-shelf
CRC	control reporting center
CRD	Capstone requirements document

C/S/As	commanders of combatant commands /Services/agencies
DAA	Designated Accreditation Authority
DAB	Defense Acquisition Board
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information System Agency
DISA (CFITS)	Defense Information System Agency, Center for Information Technology Standards
DISA (JITC)	Defense Information System Agency,
DISA (CFITS)	Defense Information System Agency,
DISN	Defense Information System Network
DMS	Defense Message System
DOD	Department of Defense
DODD	Department of Defense Directive
DODIIS	DOD Intelligence Information System
DOT&E	Director, Operational Test and Evaluation
DP	data system interoperability panel
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DT	developmental testing
DT&E	development testing and evaluation
DT/OT	developmental testing and operational testing
E3	electromagnetic environmental effects
ELP	estimated launch point
EMC	electromagnetic compatibility
EW	electronic warfare
FoS	family of systems
FR	foreign releasable
FY	fiscal year
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	global information grid
GIP	ground intercept point
GPS	global positioning system
HERO	hazards of electromagnetic radiation to ordnance

HNA	host-nation approval
IA	information assurance
IAP	information assurance panel
IATO	interim authority to operate
IAW	in accordance with
IBS	integrated broadcast system
ICEP	interoperability certification evaluation plan
IER	information exchange requirement
INFOSEC	information security
IO	information operations
IOC	initial operational capability
ITMRA	Information Technology Management Reform Act of 1966 (Clinger Cohen Act)
ITS	information technology systems
IPTP	interoperability policy and test panel
JCAPS	joint C4ISR architecture planning and analysis system
JCPAT	joint C4I program assessment tool
JITC	Joint Interoperability Test Command
JMETL	joint mission essential task list
JOA	joint operations area
JROC	Joint Requirements Oversight Council
JROCM	JROC memorandum
JSC	joint spectrum center
JTA	joint technical architecture
JTRS	joint tactical radio system
KPP	key performance parameters
LOB	line of bearing
L/L	longitude/latitude
LOS	line of sight
MAA	mission area analysis
MAIS	major automated information system
MASINT	measurement and signature intelligence
MCEB	Military Communications-Electronics Board
MDA	milestone decision authority
MDAP	Major Defense Acquisition Program

MEADS	Medium Extended Air Defense System
MIB	military intelligence board
MNS	mission need statement
NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NCBTS	noncombatants
NETWARS	Network warfare simulation
NIMA	National Imagery and Mapping Agency
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NITF	national imagery transmission format
NSA	National Security Agency
NSS	national security systems
O	objective
ORD	operational requirements document
OSD	Office of the Secretary of Defense
OT	operational testing
OT&E	Operational Test and Evaluation
OV-1	high-level operational concept graphics
OV-3	operational information exchange matrix
PK	public key
PKI	public key infrastructure
PM	program manager
PPS	precise positioning service
POC	point of contact
POM	program objective memorandum
PSA	principal staff assistant
R&D	research and development
RAD	Requirements and Acquisition Division
RAM	random-access memory
RDT&E	research, development, test, and evaluation
ROE	rules of engagement
S	SECRET
SAASM	selective availability anti-spoofing module
SABI	SECRET and Below Interoperability
SAMP	system acquisition master plan

SATCOM	satellite communications
SCC	Standards Coordination Committee
SCI	sensitive compartmentalized information
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SoS	system of systems
STAR	system threat acquisition report
STP	system tracking program
STT	strategy-to-task
SV-1	high-level system interface description
SWARF	senior warfighting forum
T	threshold
TADIL	tactical digital information link
TAMD	theater, air, and missile defense
TAOM	tactical air operations module
TBM	theater ballistic missile
TEMP	test and evaluation master plan
TOC	tactical operations center
THAAD	theater high altitude area defense
TRADOC	Training and Doctrine Command (US Army)
TRM	technical reference model
TS	TOP SECRET
TSABI	TOP SECRET and Below Interoperability
TV	technical view
U	unclassified
UAV	unmanned aerial vehicles
UJTL	universal joint task list
USA	United States Army
USAF	United States Air Force
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USD AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USIGS	United States Imagery and Geospatial System
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USMS	United States MASINT System
USMTF	United States Message Text Format
USN	United States Navy
USPACOM	United States Pacific Command
USSID	United States Signals Intelligence Directive
USSOCOM	United States Special Operations Command

USSOUTHCOM	United States Southern Command
USSPACECOM	United States Space Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command

## PART II--DEFINITIONS

accreditation. The process by which a NSS and ITS is evaluated for meeting security requirements to maintain the security of both the information and the information systems. A designated accreditation authority (DAA) is named for each system. Co-DAA's will accredit NSS and ITS in certain cases involving interoperability or integration of multiple systems.

Acquisition Category (ACAT). Categories established to facilitate decentralized decision making as well as execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. DOD 5000.2-R, part 1, provides the specific definition for each acquisition category (ACAT I through III).

ACAT I. A major defense acquisition program (MDAP) subject to Defense Acquisition Board oversight and estimated by the USD (AT&L) to require an eventual total expenditure of more than \$355 million in RDT&E funds, or \$2.135 billion in procurement funds measured in FY 1996 constant dollars.

ACAT IA. A major automated information system (MAIS) acquisition program that is estimated to require program costs in any single year in excess of \$30 million, total program costs in excess of \$120 million, or total life-cycle costs in excess of \$360 million (FY 1996 constant dollars).

ACAT IAC. A major automated information system acquisition program for which the DOD chief information officer (CIO) has delegated milestone decision authority (MDA) to the component acquisition executive (CAE) or component CIO. The "C" (in ACAT IAC) refers to component.

ACAT IAM. A major automated information system (MAIS) acquisition program for which the MDA is the DOD CIO.

ACAT IC. A major defense acquisition program subject for which the MDA is the DOD component head, or if delegated, the DOD component acquisition executive (CAE). The "C" refers to component.

ACAT ID. MDAP for which the MDA is USD (AT&L). The "D" refers to the Defense Acquisition Board (DAB), which advises the USD(AT&L) at major decision points.

administrative comments. Administrative comments to correct what appear to be typographical or grammatical errors.

architecture. The structure, relationships, principles, and guidelines that governs component design and evolution.

Automated Information Systems (AISs). An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, and storage of information. In INFOSEC, any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

certification. All NSS and ITS must be certified as interoperable with other NSS and ITS with which they have a requirement to exchange information. This certification process consists of three forms of capability confirmation -- first, one that addresses system interoperability requirements; second, one that addresses supportability; and third, one that addresses total life-cycle oversight of warfighter interoperability requirements. Figure 1 illustrates the two J-6 certifications and one validation discussed below.

(1) J-6 Interoperability Requirements Certification. This certification occurs prior to each acquisition milestone (0, I, II, III). The J-6 certifies MNSs, CRDs, and ORDs, regardless of ACAT level, for conformance with joint NSS and ITS policy and doctrine and interoperability standards. As part of the review process, J-6 requests assessments from the Services, DISA, and DOD agencies.

(2) J-6 Supportability Certification. The J-6 certifies to ASD (C3I) that C4ISPs, regardless of ACAT, adequately address NSS and ITS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems. As part of the review process, J-6 requests supportability assessments from DISA and DOD agencies. J-6

conducts a supportability certification for C4ISPs prior to milestone I, II, and III for submission to ASD (C3I) as part of the C4ISP review process.

(3) J-6 Interoperability System Validation. The J-6 validation is intended to provide total life-cycle oversight of warfighter interoperability requirements. The J-6 validates that the interoperability KPP derived from the set of top-level information exchange requirements (IERs) approved in the CRD (if applicable), ORD, and C4ISP was adequately tested during the DISA (JITC) interoperability test certification.

C4I Support Plans. The purpose of the C4ISP is to provide a window into a specific system development program through which can be seen any shortfalls in the intelligence support, NSS and ITS required for each phase of the system's life cycle.

Capstone Requirements Document (CRD). A document that contains capabilities-based requirements that facilitates the development of individual ORDs by providing a common framework and operational concept to guide their development. It is an oversight tool for overarching requirements for a system-of-systems or family-of-systems.

coalition interface. Any interface that passes information between one or more US NSS and ITS and one or more coalition partner NSS and ITS.

combined interface. Any interface that passes information between one or more US NSS and ITS and one or more allied NSS and ITS.

computer resources. Components physically part of, dedicated to, or essential in real time to mission performance; used for weapon system specialized training, simulation, diagnostic test and maintenance or calibration; or used for research and development of weapon systems.

critical comments. Critical comments will cause nonconcurrence in a document if comments are not satisfactorily resolved.

Defense Information Infrastructure. The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users across the range of military operations. It encompasses:

(1) Sustaining base, tactical, NSS, and ITS.

(2) Physical facilities used to collect, distribute, store, process, and display voice, data, and imagery.

(3) Applications and data engineering tools, methods, and processes to build and maintain the software that allow command and control (C2), intelligence, surveillance, reconnaissance, and mission support users to access and manipulate, organize, and digest proliferating quantities of information.

(4) Standards and protocols that facilitate interconnection and interoperation among networks.

(5) People and assets, which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

electromagnetic compatibility (EMC). The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation response. It evolves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

electromagnetic environmental effects (E3). E3 is the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including compatibility, interference; vulnerability, pulse; protection; hazards of radiation to personnel, ordnance, and volatile materials; and natural phenomena effects, of lightning and p-static.

family-of-systems. A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

global information grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security Systems, and related

Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

information assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

information exchange requirements. Information exchange requirements (IERS) characterize the information exchanges to be performed by the proposed family-of-systems (FoS), system-of-systems (SoS), or system. For CRDs, top-level IERS are defined as those information exchanges that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS (i.e., with other C/S/A, allied, and coalition systems). For ORDs, top-level IERS are defined as those information exchanges that are external to the system (i.e., with other C/S/A, allied and coalition systems). IERS identify **who** exchanges **what** information with **whom**, **why** the information is necessary, and **how** the information exchange must occur. Top-level IERS identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement.

information technology system (ITS). Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

intelligence certification. Confirmation by DIA of the availability, suitability, and sufficiency of intelligence to support a system or program. Intelligence certification also provides: (1) an assessment of the impact of a system or program on joint intelligence strategy, policy, architectural planning, and needs of the warfighter and (2) an evaluation of open systems architectures, interoperability, and compatibility for intelligence handling and intelligence-related information systems. This

certification will occur as a prerequisite for the system acquisition process and at each acquisition milestones.

interim authority to operate (IATO). Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an IATO will be made by the MCEB Interoperability Policy and Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.

interoperability. (1) The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together, and (2) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them or their users. The degree of interoperability should be defined when referring to specific cases. For the purposes of this instruction, the degree of interoperability will be determined by the accomplishment of the proposed IER fields.

Joint C4ISR Architecture Planning/Analysis System (JCAPS). DOD-approved static architecture tool for manipulating and conducting analysis of operational and systems architectures.

joint interface. A NSS and ITS interface that passes or is used to pass information between systems and equipment operated by two or more combatant commands, Services, or agencies (C/S/As).

Joint Technical Architecture. The DOD joint technical architecture (JTA) provides DOD systems with the basis for the needed seamless interoperability. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DOD systems, and its adoption is mandated for the management, development, and acquisition of new or improved systems throughout DOD. The JTA is structured into service areas based on the DOD technical reference model (TRM). The DOD TRM was developed to show which interfaces and content needed to be identified. The two main parts of the JTA are the core and annexes. The JTA core contains the minimum set of JTA elements applicable to all DOD systems to support interoperability.

JROC special interest. Programs identified by the JROC Secretary as being of interest to the JROC for oversight even though they do not meet the ACAT I cost thresholds or have been designated as ACAT ID.

key performance parameters (KPPs). Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a CRD KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC. ORD KPPs are included in the acquisition program baseline.

milestone decision authority. The individual designated in accordance with criteria established by the USD (AT&L), or by the ASD (C3I) for AIS acquisition programs, to approve entry of an acquisition program into the next phase.

milestones. Major decision points that separate the phases of an acquisition program.

mission need. A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance existing capabilities) through the use of new technologies. They are expressed in broad operational terms by the DOD components.

mission need statement (MNS). A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the concept exploration and definition phase.

National Security Systems (NSS). Telecommunications and information systems operated by the Department of Defense -- the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

network warfare simulation (NETWARS). The standard DOD approved communications simulation tool. CINCs, Services and agencies use NETWARS for all communications modeling purposes.

operational requirements document (ORD). A formatted statement-containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with milestone I.

originator. A DOD component or operational command that initiates a MNS. The originator may or may not be the sponsor.

procedural interface. The methods and procedures employed to establish an interconnection within and between systems or equipment and to transfer information within or between systems or equipment.

requirement. The need of an operational user, initially expressed in broad operational capability terms in the format of a MNS. It progressively evolves to system-specific performance requirements in the ORD.

seamless NSS and ITS environment. An electronic environment that allows data to be accessed by the warfighter without regard to physical or electronic boundaries.

Service deployment plans and fielding plans. Plans that describe the evolution from current capabilities to the full operational capability for new or modified NSS and ITS. Included are fielding schedules, plans, locations, and associated time-phased interoperability capabilities and requirements with current and planned systems of other DOD components or allies.

spectrum certification. The process by which development or procurement of communication-electronics systems, including all systems employing satellite techniques, will be reviewed and certified for system compliance with spectrum management policy, allocations, regulations, and technical standards to ensure that radio frequency spectrum is available. Additionally, the predicted degree of electromagnetic compatibility between the proposed system and other spectrum-dependent systems; and the possible need for and evaluation of the results of prototype electromagnetic compatibility testing will be determined.

spectrum management. Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

standardization approach. A statement(s), which demonstrates a commitment to use DOD, approved standards. For example, “The system must comply with applicable information technology standards contained in the DOD Joint Technical Architecture (JTA) current version.”

standards. Standards as referenced in this instruction are information technology system (ITS) standards. ITS standards include software and hardware standards for intelligence collection, data and information processing, information transfer, and information presentation/dissemination. ITS standards provide technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission or transfer. ITS standards apply during the development, testing, fielding, enhancement, and life-cycle maintenance of DOD information systems. ITS standards include trade association standards (e.g., IEEE standards), non-government national or international standards, Federal standards, military standards, and multinational treaty organization standardization agreements. They may take numerous forms including standards, handbooks, manuals, specifications, commercial item descriptions, and standardized drawings, all referred to collectively here as standards.

substantive comment. Substantive comments are provided because sections in the document appear to be or are potentially unnecessary, incorrect, incomplete, misleading, confusing, or inconsistent with other sections.